Intego NetBarrier X5

Manuel de l’utilisateur

Intego NetBarrier X5 pour Macintosh

© 2007 Intego. Tous droits réservés

Intego
www.intego.com

Ce manuel accompagne le logiciel Intego NetBarrier X5 pour Macintosh. Ce manuel et le logiciel Intego NetBarrier X5 décrit ici sont protégés par copyright, avec tous droits réservés. Ils ne peuvent être copiés, sauf disposition contraire dans votre licence de logiciel ou par autorisation écrite expresse d'Intego.

Le logiciel appartient à Intego et à ses fournisseurs, et sa structure, son organisation et son code sont propriété d'Intego et de ses fournisseurs. Les logiciels sont protégés par la loi sur les droits d'auteurs en France et les dispositions des traités internationaux.

Sommaire

1- A propos d'Intego NetBarrier X5 6

Présentation d'Intego NetBarrier X5 7
Firewall personnel 7
Antivandale 7
Protection de la vie privée 8
Supervision 9
Effacer vos traces avec Washing Machine 9

Présentation du manuel d'utilisation 10

2 - Introduction à la sécurité informatique 11

De Multiples raisons de se protéger 12
Comment un ordinateur peut-il être totalement sûr ? 13
Qu'est-ce qu'un firewall ? 13
Ami ou ennemi ? 13

Typologie des risques 14
Pourquoi pénétrer dans un ordinateur ? 14
Divers types d'attaques et d'intrusions 15

Protection de la vie privée 15

3 - Installation 17

Configuration matérielle et logicielle requise 18

Installation d'Intego NetBarrier X5 18

4 – Prise en main rapide 19

Utilisation d'Intego NetBarrier X5 20

Écran Aperçu de NetBarrier X5 20

Indicateurs de statut dans l'écran Aperçu 24

Assistant de configuration 25

Menu Intego 29

Protection par mot de passe de NetBarrier X5 30

Aide 30

5 - Les Quatre lignes de défense : Firewall 31

Règles du Firewall 32
Mode utilisateur simplifié 32
Mode utilisateur avancé 35

Création de règles avec l'Assistant 37
Nom/Comportement 39
Direction des communications 40
Service 42
Options 43
Conclusion 44

Création rapide de règles spécifiques à des services 46

Création manuelle de règles 48
Nom de la règle, historique, traçage et planification 49

Source et destination de la règle 52
Service de la règle 55
Interface de la règle 60
Actions de la règle 61
Sources, destinations, services ou interfaces en plusieurs segments 61
Suppression de source, destination, service ou interface 62

Mise en oeuvre des règles 63
Ordre des règles 63
Modification et suppression de règles 63
Menu contextuel des règles 64

Protection contre les chevaux de Troie 66

6 - Les Quatre lignes de défense : Filtres 68

Filtre de données 69
Fonctionnement du filtre de données 70
Types de données à protéger 71
Ajout de données au filtre 72
Activation, désactivation et suppression des éléments de données 75
Options du filtre de données 76

Filtres de surf 77
Filtrage des bannières 78
Filtrage des cookies 82
Masquage d'informations 85

7 - Les Quatre lignes de défense : Antivandale 86

Antivandale 87
Politiques 88
Options 91
Unification des options de politique 92

Anti-Spyware 93
Options 96
Applications : Ajout, suppression et modification de réglages 97

Stop List et Groupe de confiance 99
Informations contenues dans la Stop List/le Groupe de confiance 101
Note à propos des recherches DNS 103
Ajout d'adresses 104
Utilisation de jokers 105
Suppression d'adresses 105
Transfert d'adresses entre la Stop List et le Groupe de confiance 106
Modification d'une adresse 107
Menu Contextuel 108

8 - Les Quatre lignes de défense : Supervision 109

Historique 110
Options d'affichage de l'historique 111
Menu contextuel de la fenêtre de l'historique 115
Pause de l'historique 117
Effacement de l'historique 117
Export de l'historique 118
Filtrage des données dans la fenêtre de l'historique 120

Trafic 122
Modes d'affichage du trafic 122
Choix du type de données de trafic 126

NetBarrier Monitor 127
Préférences de NetBarrier Monitor 129
Widget NetBarrier Monitor 130
Économiseur d'écran de supervision de NetBarrier X5 131
Services 133
Réseaux 135
Whois 138
Traceroute 139
NetUpdate 143
9 - Comprendre les alertes 144
Réglages d'alertes 145
Exemples d'alertes 148
Compteur d'attaques 150
10 - Préférences et configurations 151
Préférences du modem 152
Préférences de l'historique 153
Préférences du trafic 156
Préférences de Whois 159
Options avancées 160
A propos de NetBarrier X5 161
Configurations 162
Création, modification et suppression de configurations 163
Export et import des réglages 166
Verrouillage et déverrouillage de l'interface 167
11 - Support technique 168
12 - Glossaire 171

1- A propos d’Intego NetBarrier X5

Présentation d'Intego NetBarrier X5

Intego NetBarrier X5 constitue la solution de sécurité Internet pour les ordinateurs Macintosh fonctionnant sous Mac OS X, en assurant une protection complète contre les intrusions venant d'Internet ou d'un réseau local.

NetBarrier X5 protège votre ordinateur des intrusions en filtrant constamment toute l'activité entrante ou sortante via Internet ou un réseau local. NetBarrier X5 assure la protection contre les voleurs, les pirates et les intrus, et vous avertit automatiquement en cas d'activité suspecte.

NetBarrier X5 dispose de quatre lignes de défense qui protègent votre ordinateur Macintosh et vos données contre les intrusions et les attaques.

Firewall personnel

NetBarrier X5 contient un firewall personnel qui filtre les données à leur entrée et sortie de l'ordinateur. Un jeu complet de filtres est proposé par défaut, et le mode avancé de protection personnalisée permet de créer vos propres règles.

Antivandale

L'Antivandale de NetBarrier X5 est un gardien performant pour votre ordinateur. Il surveille l'activité réseau de votre Mac, à la recherche de signes d'intrusion. En cas de détection d'activité suspecte, NetBarrier X5 arrête l'intrus et envoie une alerte. L'Antivandale dispose d'une fonction performante, la Stop List, qui enregistre les adresses des intrus qui tentent de pénétrer dans votre Mac, assurant ainsi leur blocage permanent. Plusieurs options sont relatives au type de protection souhaitée sur l'ordinateur.

Politiques

NetBarrier X5 arrête toutes les données entrantes considérées comme hostiles. Il peut afficher une alerte, indiquant la raison du blocage des données et demandant de permettre ou refuser leur entrée. D'autres options sont disponibles, en cas d'alerte : l'émission d'un signal sonore, la mise automatique de l'hôte dans la Stop List ou l'envoi d'un courrier électronique aux adresses choisies.

Stop List

Quand NetBarrier X5 détecte un intrus tentant de pénétrer dans votre Mac, il propose de le mettre dans la Stop List, où son adresse réseau sera enregistrée. Si un ordinateur ayant la même adresse essaie à nouveau de pénétrer dans votre ordinateur, il est automatiquement bloqué.

Groupe de confiance

Dans certains cas, des ordinateurs connus – des amis, non pas des ennemis – sont bloqués par NetBarrier X5. Il peut s'agir d'ordinateurs sur votre réseau local, bloqués suite à l'envoi de pings à votre ordinateur, par exemple. NetBarrier X5 propose de les placer dans le Groupe de confiance, où ils seront considérés comme des amis aussi longtemps que vous le souhaitez, ce qui assure leur libre accès à votre Mac. Il est important de noter que le Groupe de confiance s'applique seulement aux fonctions Antivandale de NetBarrier X5, les règles de Firewall restant appliquées aux ordinateurs du Groupe de confiance.

Anti-Spyware

NetBarrier X5 permet le contrôle de l'accès Internet et réseau, individualisé par application. Chaque fois qu'une application qui n'est pas digne de confiance tente de se connecter à un réseau, NetBarrier X5 peut afficher une alerte, précisant l'application concernée. Vous pouvez alors autoriser l'accès au réseau, s'il s'agit vraiment d'une application amenée à utiliser le réseau. Cependant, si une application essaie de se connecter secrètement, vous pouvez la bloquer de façon permanente.

Protection de la vie privée

NetBarrier X5 aide à la protection des informations liées à la vie privée. Il filtre les données pour assurer qu'aucune information sensible ne quitte votre ordinateur, il bloque les bannières publicitaires et il permet la navigation de manière anonyme. Une fonction importante sait cacher des informations concernant l'ordinateur : la plate-forme, le navigateur utilisé, et la dernière page web visitée.

Supervision

NetBarrier X5 dispose d'outils performants assurant la supervision de l'activité réseau. Les compteurs d'activité présentent le trafic réseau en temps réel, et les fonctions complémentaires de supervision proposent des informations importantes relatives à l'ordinateur, son réseau, ainsi que les services et connexions actifs.

NetBarrier X5 propose même un programme séparé, NetBarrier Monitor, que vous pouvez laisser ouvert en permanence, ainsi qu'un économiseur d'écran de supervision, qui vous permet d'avoir constamment un oeil sur l'activité réseau.

Effacer vos traces avec Washing Machine

NetBarrier X5 inclut un programme séparé, Washing Machine, qui complète la protection de votre vie privée en vous aidant à effacer les informations relatives à vos habitudes sur Internet. Ce programme facilite la façon de supprimer les signets, les cookies, les caches, les historiques de téléchargement et les historiques de navigation pour quelques dizaines de programmes qui stockent régulièrement ces types d'informations ; il peut être réglé pour le "nettoyage" périodique de ces éléments, ce qui allège le processus de protection.

Washing Machine regroupe des fonctions précédemment inclues dans NetBarrier ; vous pouvez lancer le programme à partir du menu Intego, dans le sous-menu NetBarrier X5. Pour des informations détaillées relatives à Washing Machine, consultez le Manuel utilisateur d'Intego Washing Machine, reçu avec NetBarrier X5.

Présentation du manuel d'utilisation

Selon votre profil :	**Nous vous conseillons la lecture des chapitres suivants :**
Vous êtes connecté à Internet chez vous	• Chapitre 2, **Introduction à la sécurité informatique** • Chapitre 3, **Installation** • Chapitre 4, **Prise en main rapide** • En option : Chapitres 5-8, **Les Quatre lignes de défense** NetBarrier X5 est configuré pour la protection automatique de votre ordinateur contre les intrusions.
Vous êtes un utilisateur universitaire ou professionnel, connecté à un réseau local et à Internet	• Chapitre 2, **Introduction à la sécurité informatique** • Chapitre 3, **Installation** • Chapitre 4, **Prise en main rapide** Les modes de protection de base de NetBarrier X5 sont sans doute suffisants ; cependant, vous pourriez lire également les chapitres 5-8, **Les Quatre lignes de défense**
Vous êtes un utilisateur avancé et vous utilisez l'ordinateur en tant que serveur, ou vous administrez un réseau	Tout le manuel vous concerne, mais penchez-vous surtout sur les chapitres 5-8, **Les Quatre lignes de défense**, et particulièrement le chapitre 5 pour découvrir la création de règles particulières.

Un glossaire en fin de manuel définit des termes spécifiques.

2 - Introduction à la sécurité informatique

De Multiples raisons de se protéger

Vous utilisez votre Mac dans le cadre professionnel ou simplement pour naviguer sur Internet, vous êtes en ligne toute la journée, ou simplement de temps en temps, vous êtes sur un réseau local dans un bureau chez vous, ou bien membre d'une grande entreprise ou d'une université : quel que soit le contexte, votre ordinateur contient des informations sensibles. Cela va des numéros de cartes de crédit aux données de comptes bancaires, des contrats avec vos clients ou vos employés, des projets confidentiels ou des messages électroniques aux mots de passe. Quelles que soient les données sensibles dans votre Mac, elles peuvent intéresser quelqu'un.

Quand vous utilisez le Mac pour des activités régulières, qu'elles soient personnelles ou professionnelles, il est fortement conseillé de protéger les informations contenues.

Considérez l'ordinateur comme une maison. En sortant, vous prenez soin de verrouiller portes et fenêtres, mais protégez-vous votre Mac de la même façon ? Dès lors que vous êtes connecté à un réseau, des pirates rusés ou des criminels informatiques ont un moyen d'y pénétrer - à moins de mettre en oeuvre la défense assurée par NetBarrier X5.

Quand votre Mac est connecté à un réseau, que ce soit un réseau local privé ou Internet, il est comme une maison. NetBarrier X5 agit comme un verrou protégeant portes et fenêtres. Vous n'avez aucun moyen de savoir qui vous surveille quand vous êtes connecté à un site web. Peut-être que ce site de jeu, avec les « tuyaux » que vous recherchez, cache un pirate, prêt à sauter sur votre Mac, pour y dénicher quelque chose d'intéressant. Ou bien ce site d'informations boursières, où rechercher des résultats d'entreprises, cache un pirate curieux, aimant bien semer la pagaille dans les ordinateurs, juste pour s'amuser.

Sans Intego NetBarrier X5, vous ne saurez même pas qu'on tente de pénétrer dans votre Mac.

Un ordinateur n'est en sécurité que dans la mesure où les personnes qui y ont accès sont dignes de confiance. NetBarrier X5 le protège en évitant tout accès réseau non autorisé et toute exportation non autorisée d'informations sensibles.

Comment un ordinateur peut-il être totalement sûr ?

On dit que le seul ordinateur qui soit totalement en sécurité est celui qui est éteint et débranché, enfermé dans un coffre-fort recouvert de titane, enterré dans un bunker en béton et entouré de gaz neurotoxique et de gardes armés jusqu'aux dents. Évidemment, ce n'est pas très pratique : si vous avez un ordinateur, vous voulez vous en servir.

NetBarrier X5 assure un niveau de protection qui dépasse les besoins de la plupart des utilisateurs ; de plus, il s'agit d'un outil performant pour les administrateurs de réseau et de système grâce à ses règles paramétrables, permettant d'adapter la protection aux besoins spécifiques.

Qu'est-ce qu'un firewall ?

Un firewall est comme un mur. Il protège l'ordinateur ou le réseau en séparant les utilisateurs en deux groupes : ceux situés à l'intérieur du mur, et ceux situés à l'extérieur. Il est configuré pour déterminer l'accès dont bénéficient les usagers extérieurs aux ordinateurs situés à l'intérieur du mur, et celui que les usagers intérieurs ont aux ordinateurs et aux réseaux de l'autre côté du mur.

Un firewall est une sorte de filtre entre l'ordinateur, ou le réseau, et un réseau élargi, comme l'Internet. Il agit par filtrage des paquets de données, et examen de leur origine et de leur destination.

NetBarrier X5 offre une protection firewall efficace pour votre Mac et, grâce à la protection personnalisée, les utilisateurs avancés peuvent configurer des règles spécifiques contre des ennemis qui tenteraient d'infiltrer l'ordinateur.

Ami ou ennemi ?

Un mur doit offrir une voie de circulation. L'Antivandale de NetBarrier X5 agit comme un filtre, ou un garde devant la porte du mur, vérifiant toutes les données entrantes et sortantes à la recherche de signes révélant des pirates, des crackers, des vandales, des espions, des intrus et des voleurs. Cette opération est possible car il existe de nombreuses méthodes "standard" de pénétrer dans un ordinateur non protégé, et NetBarrier X5 connaît ces méthodes.

Typologie des risques

Pourquoi pénétrer dans un ordinateur ?

Il y a de nombreuses raisons d'entrer dans un ordinateur. Quelquefois, c'est simplement le moyen d'accéder à un nombre croissant de systèmes ; en sautillant entre plusieurs ordinateurs avant de pénétrer dans un nouvel ordinateur, le pirate espère égarer ses poursuivants et dissimuler sa trace. Il a intérêt à forcer l'entrée du plus grand nombre possible de sites différents, afin de « blanchir » ses connexions.

Certaines personnes adorent jouer avec les ordinateurs et les amener aux limites de leurs capacités. C'est un peu comme ceux qui couvrent les murs de graffiti : ils le font simplement pour l'exploit.

Mais les envahisseurs les plus sérieux sont de vrais criminels. Il peut s'agir de concurrents, à la recherche d'informations sur les activités, les projets ou les clients d'une entreprise ; de voleurs, à la recherche de mots de passe et de numéros de cartes de crédit ; ou tout simplement d'espions. Alors que la plupart des sociétés ont une stratégie de sécurité informatique, peu d'entre elles pensent à protéger les données contenues dans les ordinateurs personnels de leurs employés ; pourtant, ces ordinateurs contiennent souvent des fichiers sensibles que ces derniers ont ramenés de leur lieu de travail.

Nous vivons malheureusement dans un monde où toute chose de valeur est une cible pour les voleurs. Comme notre économie est bâtie autour de l'information, celle-ci est bien évidemment devenue une cible de choix. Un simple exemple : l'an dernier, vous avez fait livrer des fleurs à votre mère, pour son anniversaire. Vous avez commandé par télécopie, parce que vous ne vous souhaitiez pas envoyer votre numéro de carte de crédit sur le web. Mais le fichier que vous avez tapé, contenant ce numéro de carte, est toujours sur le disque dur. Si quelqu'un le trouvait, il pourrait en disposer et vous risqueriez d'être la victime d'une fraude.

Divers types d'attaques et d'intrusions

De multiples raisons conduisent à tenter d'accéder à l'ordinateur d'autres personnes, et de nombreuses méthodes existent. Voici quelques exemples :

- Voler des fichiers ou des informations confidentiels.
- Exécuter des commandes informatiques qui modifient le système, effacent le disque dur ou rendent l'ordinateur inutilisable.
- Changer le contenu des sites web par malveillance.
- Lancer des attaques de déni de service qui peuvent rendre un ordinateur provisoirement inutilisable.
- Obtenir des informations à propos d'un ordinateur, qui permettront ultérieurement de forcer l'entrée dans un réseau ou un ordinateur.

Protection de la vie privée

Vous ne le remarquez pas quand vous surfez sur Internet, mais divers sites web essaient de vous soutirer une quantité impressionnante d'informations personnelles. Il est facile d'identifier ceux qui demandent très clairement de vous enregistrer avant utilisation ; vous entrez un nom d'utilisateur et un mot de passe et, quelquefois, vos nom et adresse ainsi que d'autres données. Ces informations servent souvent à suivre la trace du comportement des internautes, pour découvrir les centres d'intérêts et proposer des produits ou des services.

De plus en plus d'internautes refusent de communiquer ce type d'informations aux sites web. Quelquefois vous apprenez à vos propres dépens : vous vous enregistrez sur un site web, et voilà que vous recevez du « spam », des courriers électroniques indésirables, des messages concernant des produits que vous n'avez jamais sollicités. À ce moment-là, c'est déjà trop tard.

Les sites web disposent cependant d'autres moyens d'obtenir des informations. Saviez-vous que votre navigateur envoie des informations aux sites web concernant le système d'exploitation ou le type de navigateur, et même la dernière page web visitée ?

Ensuite viennent les cookies. Un cookie est un fichier sur le disque dur, contenant des informations envoyées par un serveur web à un navigateur web, qui sont ensuite renvoyées par le navigateur chaque fois qu'il accède à ce serveur. Généralement, le cookie sert à authentifier ou identifier un utilisateur enregistré sur un site web sans lui demander de s'identifier à chaque passage. Il peut servir à maintenir le « panier » des marchandises choisies lors d'une session d'achat sur un site, affiner les réglages d'un site (présenter des pages différentes selon les utilisateurs), ou suivre la trace d'accès des divers utilisateurs.

Alors que les cookies peuvent être d'un usage légitime, certains sites web indélicats en profitent pour rassembler des données sur vos habitudes de navigation. Ces données sont ensuite vendues à des sociétés qui vous contactent directement à propos de produits ou de services spécifiques, correspondant à ces habitudes, ou qui vont même jusqu'à vous présenter des bannières publicitaires ciblées, quand vous surfez sur certains sites.

NetBarrier X5 a une approche très simple de la protection de la vie privée : le programme vous donne les moyens d'éviter que certains types d'informations soient enregistrés à votre insu.

3 - Installation

Configuration matérielle et logicielle requise

- Tout ordinateur compatible Mac OS X (supporté officiellement par Apple)
- Mac OS X 10.4 ou ultérieur, ou Mac OS X Serveur 10.4 ou ultérieur
- 40 Mo d'espace libre sur disque dur

Installation d'Intego NetBarrier X5

Pour les informations relatives à l'installation et la sérialisation d'Intego NetBarrier X5, consultez le Manuel de Démarrage Intego, inclus avec votre copie du programme. Si vous avez acheté Intego NetBarrier X5 par téléchargement sur le site web d'Intego, ce manuel se trouve dans l'image disque qui contient le logiciel. Si vous avez acheté NetBarrier X5 sur un CD ou un DVD, ce manuel se trouve sur le disque.

4 – Prise en main rapide

Utilisation d'Intego NetBarrier X5

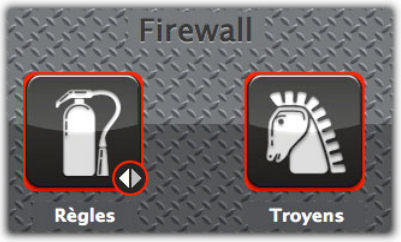
Quand vous ouvrez NetBarrier X5 pour la première fois, l'écran Aperçu apparaît. Si vous avez déjà utilisé une version précédente de NetBarrier, vous pouvez noter que cet écran a été simplifié et optimisé. N'ayez aucune inquiétude : vous allez retrouver toutes les fonctionnalités.

Écran Aperçu de NetBarrier X5

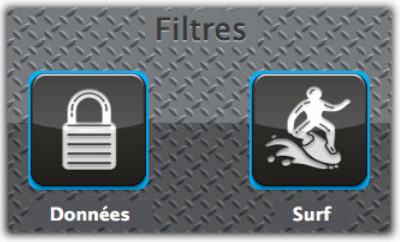
L'écran Aperçu donne l'accès rapide à divers éléments :

- Les fonctions, réglages et historiques de NetBarrier X5,
- Plusieurs utilitaires de réseau, tels que Whois et Traceroute,
- Des indicateurs visuels précisant les types de protection activés,
- Des informations sur le programme lui-même, dont la date de dernière mise à jour,
- Accès aux multiples configurations, pour pouvoir modifier rapidement les réglages de protection.

Au centre de l'écran Aperçu, on trouve les sections contrôlant les quatre lignes de défense de NetBarrier X5. Les contrôles pour le Firewall, l'Antivandale et les Filtres sont figurés par les gros boutons au cœur de l'écran Aperçu ; les contrôles pour la Supervision sont les boutons plus petits dans le coin inférieur droit.



La section Firewall donne accès aux Règles qui définissent les programmes pouvant échanger des informations via votre Mac, et aux réglages des Troyens pour protéger votre Mac contre les chevaux de Troie nuisibles.



La section Filtres donne accès aux réglages évitant l'envoi de données spécifiques sur Internet et les réseaux locaux, et bloque certains types d'informations qui sont échangés quand vous surfez sur Internet.

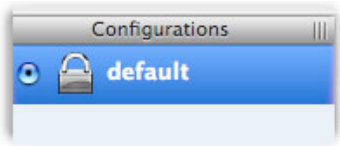
La section Antivandale donne accès à vos Politiques dans l'arrêt de certains types d'attaques ; accès au mode de protection contre les programmes qui se connectent en secret aux ordinateurs distants (Anti-Spyware) ; à votre Stop List, qui garde trace des "méchants" ; et à votre Groupe de confiance, pour les amis qui ont explicitement accès à votre Mac.

Vous avez accès aux fonctions de Supervision via des boutons en bas à droite de l'écran Aperçu. Ils sont également disponibles via des sélections sous le menu Affichage, et à l'aide de raccourcis de clavier. Les boutons de supervision sont les suivants :

	Historique	Option-Commande-L	Enregistrement des activités de NetBarrier, et trafic entrant et sortant de votre Mac, sur Internet ou des réseaux locaux.
	Trafic	Option-Commande-1	Trafic réseau entrant et sortant de votre Mac.
	Services	Option-Commande-2	Liste des services réseaux disponibles à partir de votre Mac.
	Réseaux	Option-Commande-3	Réseaux extérieurs qui sont actuellement disponibles à votre Mac.
	Whois	Option-Commande-4	Informations relatives aux propriétaires et gestionnaires de domaines sur Internet.
	Traceroute	Option-Commande-5	Chemin sur le réseau, emprunté par un signal pour aller de votre Mac à un autre ordinateur.

Chacune de ces fonctionnalités est décrite au chapitre 8, **Les Quatre lignes de défense : Supervision**.

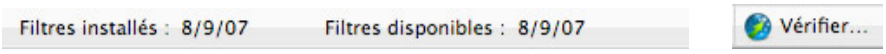
À gauche de la fenêtre Aperçu, se trouve une liste de Configurations. Chaque configuration est un ensemble de réglages pour la protection Firewall, Filtres et Antivandale de NetBarrier. Au début, il n'existe qu'une seule configuration, nommée "défaut". Le bouton radio indique la configuration active.



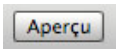
Au bas de la liste des Configurations, on trouve quatre boutons permettant de dupliquer, modifier, supprimer et masquer les configurations. (Vous basculez entre l'état affiché ou masqué de la liste en

appuyant sur Commande-K ou en choisissant Présentation > Masquer/Afficher la liste des Configurations.) Pour en savoir plus, reportez-vous au chapitre 10, **Préférences et configurations.**

Tout en haut de l'écran, on trouve la barre de statut de NetUpdate, indiquant la date des derniers filtres NetBarrier installés sur votre Mac, et la date des derniers filtres disponibles via Intego NetUpdate. NetUpdate vérifie périodiquement les mises à jour, ou vous pouvez vérifier immédiatement, en cliquant sur le bouton « Vérifier...» dans le coin supérieur gauche. Pour masquer la barre de statut, sélectionnez Présentation > Masquer la barre de statut NetUpdate. Pour en savoir plus, reportez-vous au Manuel utilisateur de NetUpdate.

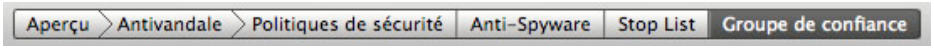


Enfin, un petit bouton en haut à gauche de l'écran Aperçu indique la section de l'interface de NetBarrier X5 actuellement affichée. Quand vous ouvrez NetBarrier X5 pour la première fois, ce bouton indique seulement Aperçu.



Cependant, quand vous consultez l'écran de contrôle des chevaux de Troie, par exemple, le bouton apparaît segmenté, indiquant clairement qu'il s'agit d'une partie de la section Firewall, ainsi que les Règles.

En cliquant sur Règles, vous vous déplacez vers les règles ; en cliquant sur Firewall ou Aperçu, vous revenez à l'écran Aperçu. Les sections Filtres et Antivandale fonctionnent de la même façon.



Indicateurs de statut dans l’écran Aperçu

Le statut de diverses fonctionnalités de NetBarrier X5 apparaît intégré aux icônes dans l’écran Aperçu. Quand les sections Troyens, Données et Anti-Spyware sont activées, on constate un petit signe de cochage dans le coin inférieur droit de leurs icônes.

Désactivé	Activé

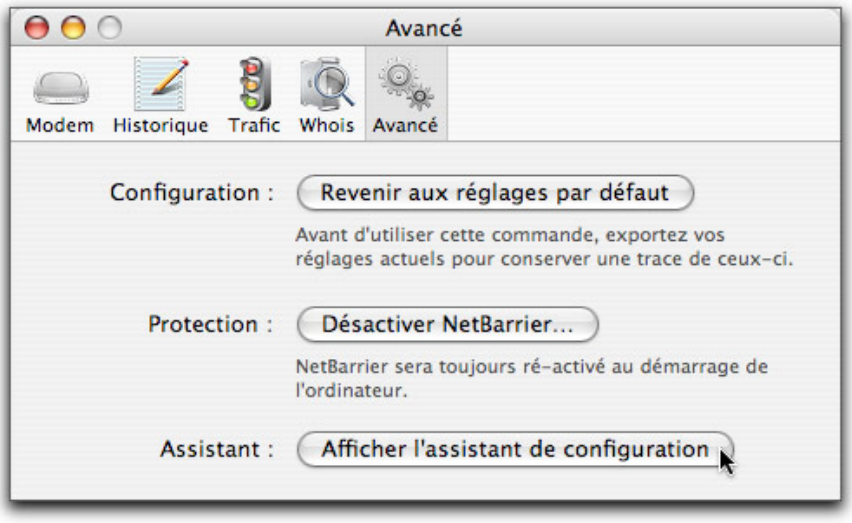
De même, les icônes de la Stop List et du Groupe de confiance indiquent le nombre d’entrées dans leurs listes respectives.

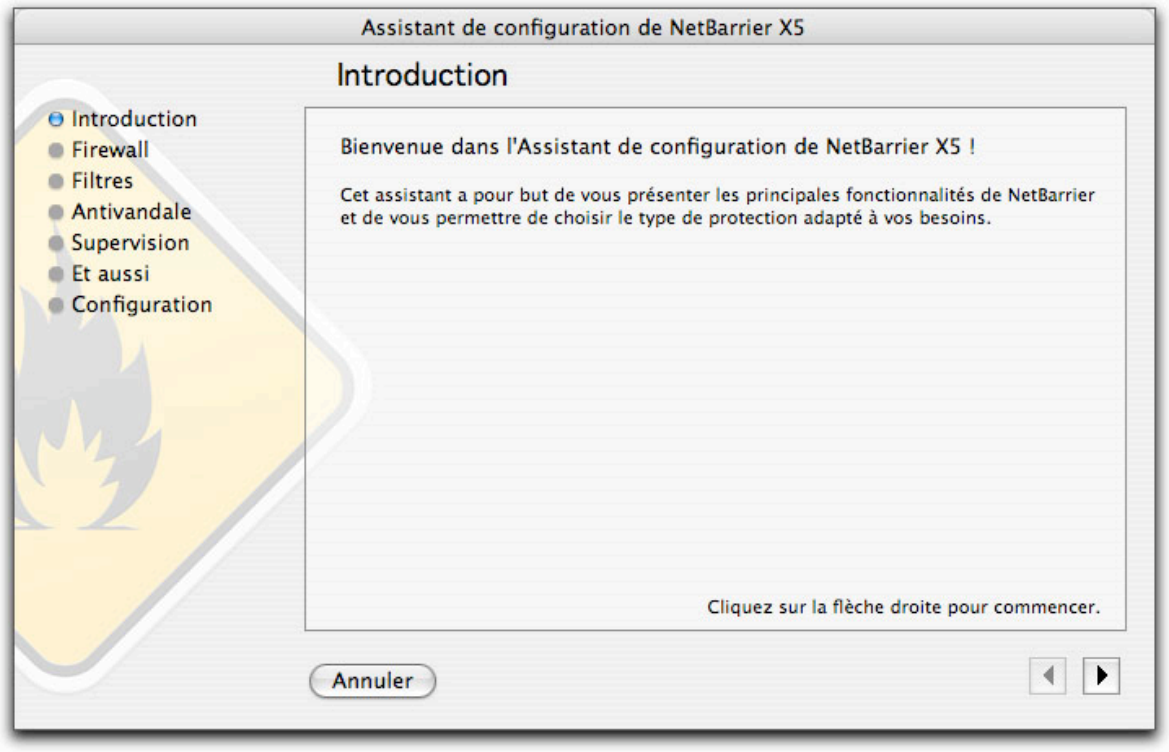
Aucune entrée	Deux entrées

Assistant de configuration

Quand vous installez NetBarrier X5 et redémarrez votre Macintosh, le logiciel commence automatiquement à protéger l'ordinateur. Le firewall est lancé en mode Client, serveur local et l'activité est enregistrée dans l'historique. Dans ce mode, l'activité entre votre Mac et Internet est possible, comme client, et votre Mac peut fonctionner à la fois en client et serveur sur un réseau local. Pour plus d'informations, reportez-vous plus bas aux modes de Firewall de NetBarrier X5.

NetBarrier X5 inclut un assistant de configuration qui vous aide à optimiser les réglages de base selon votre usage du réseau. À la première ouverture de NetBarrier X5, l'Assistant de configuration est lancé automatiquement. Si vous procédez à la mise à niveau d'une ancienne version de NetBarrier, vous devez lancer manuellement l'Assistant de configuration. Pour cela, sélectionnez NetBarrier X5 > Préférences et cliquez sur le bouton Avancé. Cliquez sur Afficher l'assistant de configuration au bas du panneau. Un mot de passe administrateur est nécessaire pour lancer l'Assistant de configuration.





Cliquez sur la flèche droite pour commencer la configuration de NetBarrier X5. En cliquant sur la flèche gauche, vous revenez aux écrans précédents. L'Assistant de configuration de NetBarrier X5 présente brièvement des écrans d'informations relatives aux différentes fonctions :

- **Firewall (Règles et Troyens)**
- **Filtres (protection des données et de la navigation)**
- **Antivandale (Politiques, Anti-Spyware, Stop List et Groupe de confiance)**
- **Supervision (Historique et cinq outils de supervision)**
- **Et aussi (divers outils)**

Quand c'est terminé, l'écran Configuration permet la sélection de la configuration voulue de NetBarrier X5.

Les configurations sont les suivantes :

Nom	Choix optimal si…	Réglage du Firewall	Autres réglages
Défaut	…vous avez besoin de permettre l'accès à votre Mac depuis le réseau local, mais avec protection contre les intrusions depuis des ordinateurs situés hors de votre réseau local.	Mode "Client, serveur local" : l'activité entre votre Mac et Internet est possible, comme client, et votre Mac peut fonctionner à la fois en client et serveur sur un réseau local.	Tous les filtres de protection et Antivandale sont désactivés.
Normal	…vous n'utilisez pas votre ordinateur comme serveur de réseau ou en partage local de fichiers.	Mode client : votre Mac peut fonctionner seulement comme client sur un réseau local ou sur Internet. Les	Les filtres Antivandale sont activés contre les attaques par dépassement de buffer, les tentatives

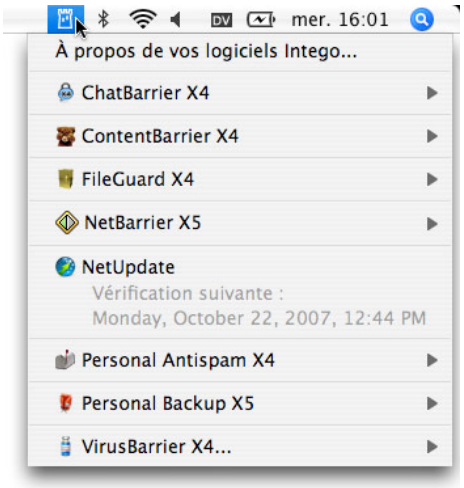
		fonctions serveur de l'ordinateur sont bloquées.	d'intrusion, les attaques Ping, les Port Scans et le SYN Flooding, mais désactivés contre les Pings broadcast. Tous les filtres de protection sont désactivés.
Fort	…vous voulez une protection maximale, et vous pouvez accepter que cette configuration risque de bloquer certains trafics.	Mode client.	Tous les filtres Antivandale sont activés, de même que ceux protégeant contre les Troyens.

Cliquez sur le bouton Configurer pour activer la configuration sélectionnée.

Menu Intego

NetBarrier X5, comme tous les autres logiciels Intego, installe un menu spécifique dans la barre de menus, appelé le menu Intego. Son icône est une petite tour, comme dans le logo Intego.

Cliquez sur l'icône du menu Intego pour afficher le menu présentant tous vos logiciels Intego :



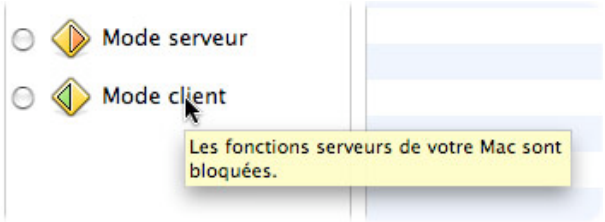
Depuis le menu Intego, vous pouvez modifier plusieurs des réglages de NetBarrier X5. Sélectionnez le menu Intego > NetBarrier X5. Vous pouvez changer de configuration, et vous pouvez activer ou désactiver des réglages, tels que les réglages de filtrage ou de type de filtre. Vous pouvez ouvrir Intego Washing Machine depuis le menu Intego, choisissez le menu Intego, puis NetBarrier X5 > Ouvrir Washing Machine.... Pour ouvrir NetBarrier Monitor, choisissez NetBarrier X5 > Ouvrir NetBarrier Monitor.

Protection par mot de passe de NetBarrier X5

NetBarrier X5 utilise la protection par mot de passe intégrée à Mac OS X. Pour installer et configurer le programme, l'utilisateur doit disposer des droits d'administrateur, et se connecter avec l'identifiant et le mot de passe d'un administrateur. Les utilisateurs qui ne disposent pas de droits d'administrateur ne peuvent modifier aucun des réglages et préférences de NetBarrier X5. Ces utilisateurs peuvent consulter les fonctions de supervision, comme les historiques et les compteurs d'activité, mais ils ne sont pas autorisés à modifier le fonctionnement du programme.

Aide

L'aide concernant certaines fonctions de NetBarrier X5 est disponible en maintenant le curseur sur certains textes et zones :



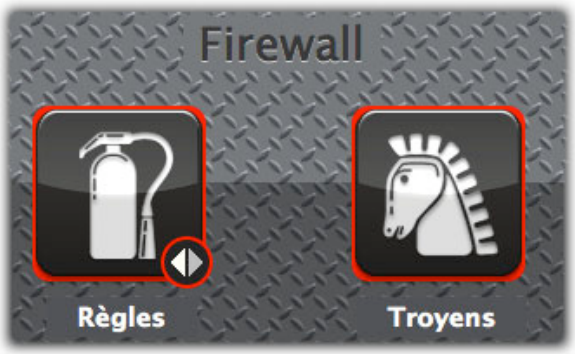
Une info-bulle apparaît, expliquant les diverses fonctionnalités.

Pour une aide complète, ce manuel est disponible en choisissant Aide > Manuel de l'utilisateur de NetBarrier X5.

5 - Les Quatre lignes de défense : Firewall

NetBarrier X5 est un programme performant et convivial qui protège votre Mac lors de la connexion à un réseau, via quatre lignes de défense. La première ligne est un firewall personnel, qui est un outil de filtrage des paquets de données échangées entre l'ordinateur et Internet ou un réseau TCP/IP local. Il protège également contre les chevaux de Troie en bloquant les ports spécifiques utilisés.

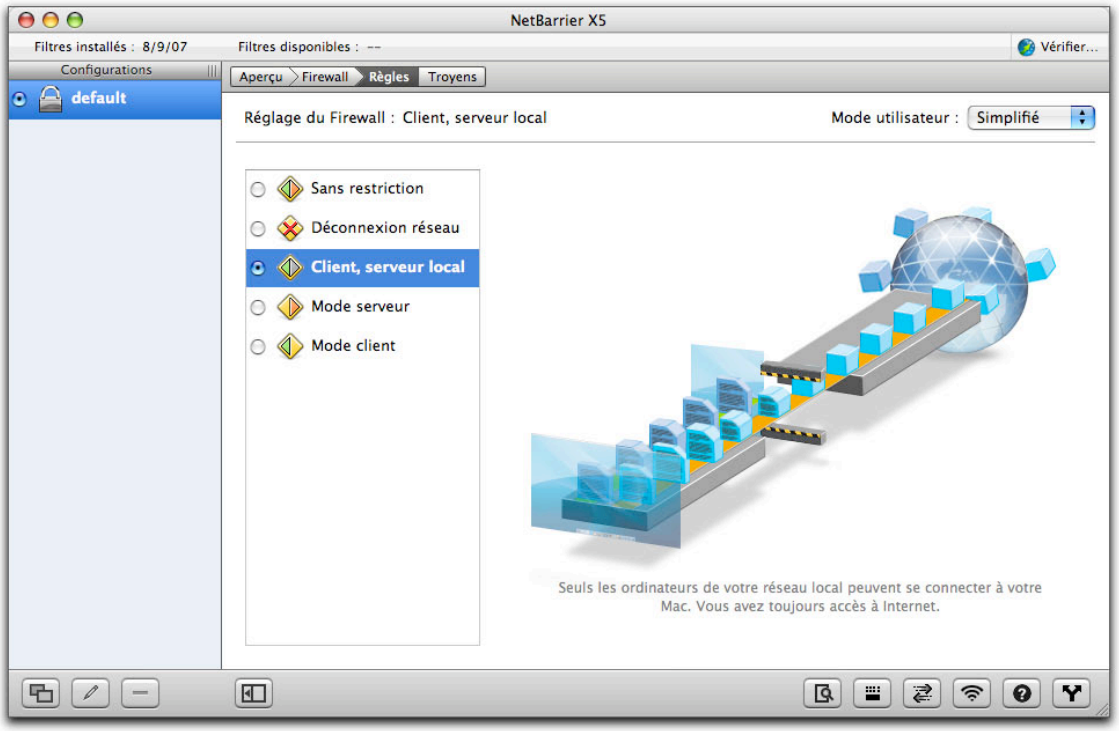
L'écran Aperçu présente la section Firewall, contenant deux boutons : Règles et Troyens.



Règles du Firewall

Mode utilisateur simplifié

Quand vous cliquez sur le bouton Règles, NetBarrier X5 présente le mode simplifié de contrôle des réglages du Firewall. Les cinq réglages préfixés couvrent toutes les situations rencontrées en usage normal ; chacun est accompagné d'une animation expliquant l'effet de son application. L'écran le plus proche de vous représente votre Mac ; le globe représente l'Internet ; l'écran intermédiaire représente la limite de votre réseau local. Ici, le réglage par défaut, "Client, serveur local", indique comment votre ordinateur peut recevoir des informations venant d'au-delà du réseau local, mais que les ordinateurs au-delà de votre réseau local ne peuvent pas avoir accès à votre Mac.



Les cinq réglages du firewall, et leur apparence sur l'écran Aperçu, sont présentés ci-après :

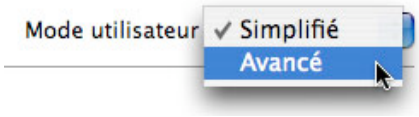
Sans restriction	Le firewall de NetBarrier X5 permet l'échange de toutes les données entrantes et sortantes.
Déconnexion réseau	Le firewall de NetBarrier X5 empêche tout échange de données entre l'ordinateur et Internet ou un réseau TCP/IP local. Ce réglage est utile si vous vous éloignez de l'ordinateur et vous souhaitez le protéger totalement.
Client, serveur local	Le firewall de NetBarrier X5 permet le fonctionnement de votre Mac comme client et comme serveur sur un réseau local. L'activité entre votre Mac et Internet est possible, à la fois comme ordinateur client et serveur sur un réseau local.
Mode serveur	Le firewall de NetBarrier X5 permet le fonctionnement de votre Mac seulement comme serveur : toutes les fonctions client, y compris votre capacité à surfer sur Internet, sont bloquées.
Mode client	Le firewall de NetBarrier X5 permet le fonctionnement de votre Mac seulement comme client sur un réseau local ou sur Internet. Les fonctions serveur et partage de fichier de votre Mac sont bloquées.

Ces cinq réglages sont suffisants pour la plupart des utilisateurs. Cependant, si vous voulez plus de contrôle sur l'accès à votre ordinateur – si, par exemple, vous êtes meneur de jeu et vous voulez interdire tout trafic excepté les communications faisant partie du jeu – vous avez alors besoin du mode avancé de NetBarrier X5.

Mode utilisateur avancé

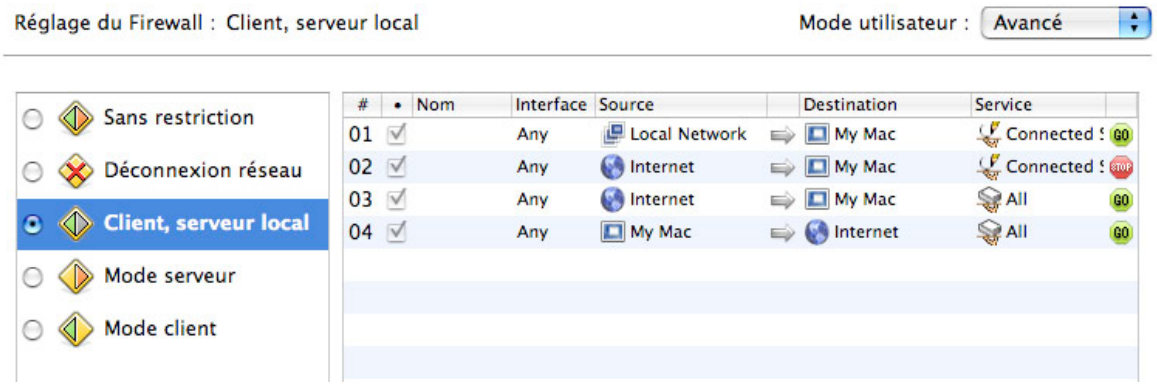
Chacun des cinq réglages décrits ci-dessus est constitué d'un ensemble de règles ; chacune de ces règles est définie en nommant les sources, les destinations, les services et les interfaces autorisés ou interdits. Le mode simplifié ne vous permet pas de changer de règles ni de modifier l'un de leurs éléments. Pour cela, vous devez passer au mode avancé de l'écran Firewall.

Pour accéder au jeu complet des règles du firewall de NetBarrier X5, cliquez sur le menu déroulant Mode utilisateur dans le coin supérieur droit et passez de Simplifié à Avancé.



ATTENTION : La modification de ces réglages pourrait fortement affecter la capacité d'accès de votre ordinateur aux réseaux locaux et à Internet. Nous vous conseillons de bien maîtriser les effets et le fonctionnement du mode avancé avant de l'utiliser.

En mode simplifié, une animation apparaît quand vous cliquez sur l'un des cinq réglages du firewall ; en mode avancé, vous avez accès aux détails de chaque réglage.



Dans cet exemple, le réglage "Client, serveur local" contient quatre règles. La première règle permet l'accès du réseau local à votre Mac via tous les "Services connectés" - c'est-à-dire, les connexions TCP concernant des communications en va-et-vient, telles que la distribution de fichiers venant de votre Mac. La seconde règle, cependant, interdit de telles connexions venant de l'Internet au sens large, ce qui évite que votre Mac agisse comme serveur pour un ordinateur inconnu hors de votre réseau local. La troisième règle permet toutes les autres communications venant d'Internet vers votre Mac, tandis que la quatrième permet toutes les communications de votre Mac *vers* Internet.

Les cinq réglages du firewall sont préfixés et "gelés" dans un objectif de facilité et de stabilité : vous ne pouvez pas modifier leurs règles, ni leur ordre d'affichage. Cependant, en mode avancé, NetBarrier X5 propose deux façons de créer des réglages personnalisés et additionnels : via l'Assistant et manuellement.

Dans chaque cas, la première étape est de cliquer sur le bouton **+** sous la liste des réglages. Un nouveau réglage apparaît, intitulé "réglage sans titre". Cliquez sur ce réglage et tapez le nom choisi, puis appuyez sur Entrer ou Retour pour rendre la modification permanente.

Note : vous avez seulement créé ce réglage, mais vous ne l'avez **pas** encore activé. Nous vous conseillons de ne pas activer les réglages du firewall avant d'avoir fini d'ajouter toutes vos règles. Pour en faire le réglage actif, cliquez sur le bouton radio à sa gauche.

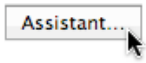
Création de règles avec l'Assistant

NetBarrier X5 contient un assistant qui vous guide dans la création des règles de firewall personnalisées. Grâce à l'assistant, la création de règles se résume à quelques clics de souris. Bien que toutes les fonctionnalités de règle de NetBarrier X5 ne soient pas disponibles dans ce cadre, la plupart des besoins relatifs aux règles de firewall sont couverts. Pour une personnalisation plus poussée, créez les règles à l'aide de l'assistant puis passez à une modification manuelle.

L'Assistant de NetBarrier X5 guide l'utilisateur dans la série d'étapes nécessaires à la création des règles :

- **Nom et Comportement**
- **Direction**
- **Service**
- **Durée de vie**
- **Options**
- **Conclusion**

Pour créer une règle à l'aide de l'assistant, cliquez sur le bouton Assistant...



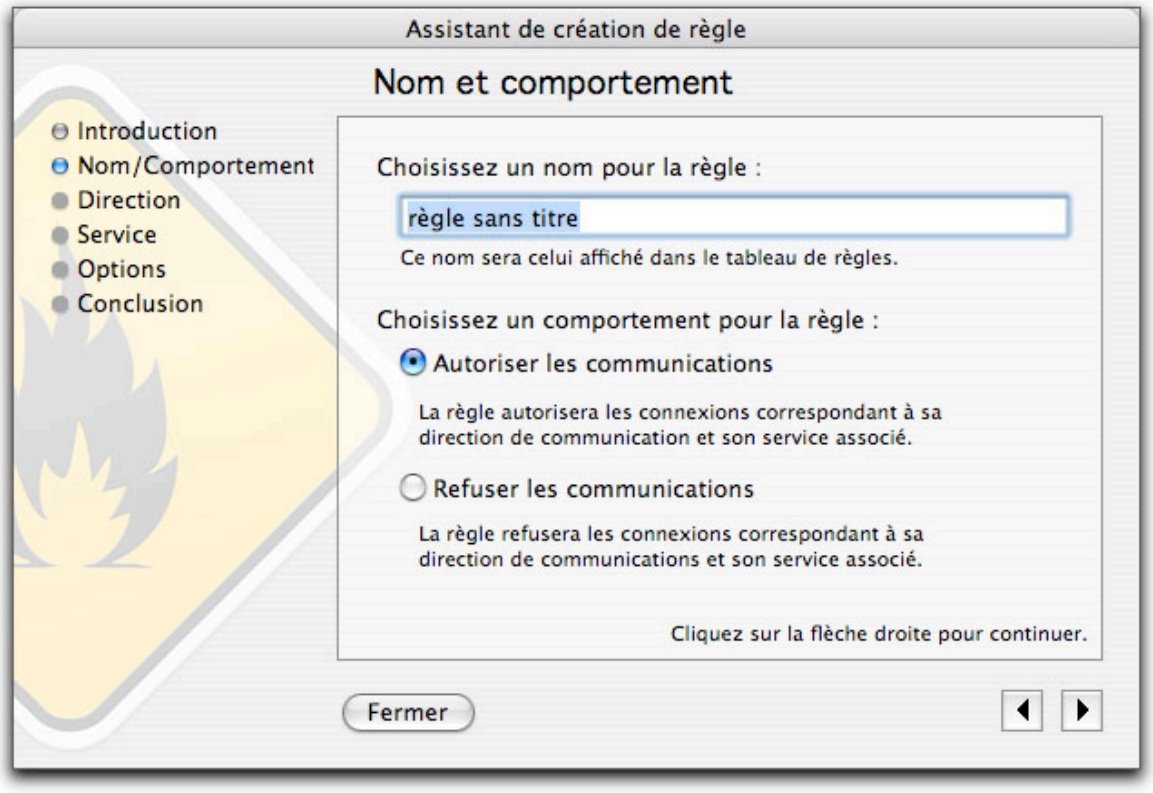
Le premier écran de l'assistant de création de règle apparaît.

Cliquez sur la flèche droite pour commencer la création. En cliquant sur la flèche gauche, vous revenez aux écrans précédents.

Cliquez sur Fermer pour quitter l'assistant.

Nom et Comportement

Cet écran permet le choix du nom et du comportement de la règle.

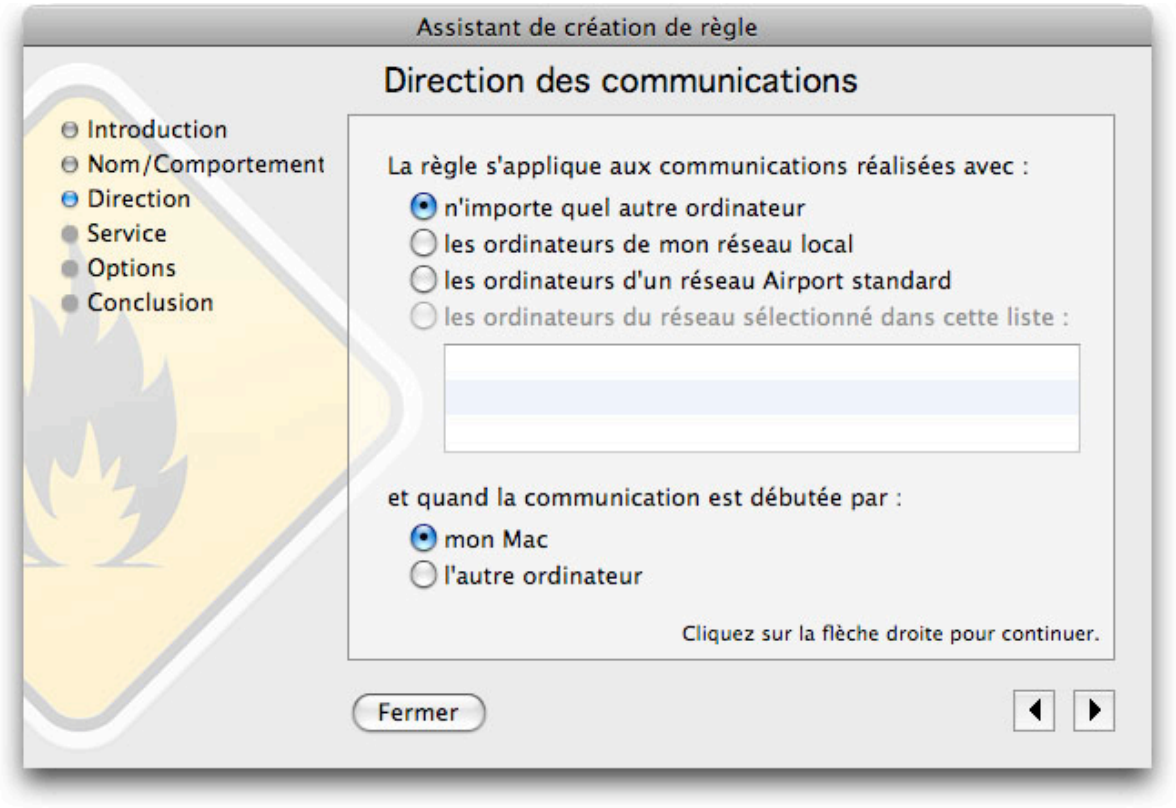


Entrez le nom de la règle dans le champ de nom, puis choisissez son comportement : Autoriser ou Refuser les communications. Si vous choisissez Autoriser les communications, la règle va autoriser le passage des données correspondant à sa direction et son service associé. Si vous choisissez Refuser les communications, la règle va refuser le passage des données correspondant à sa direction et son service associé.

Cliquez sur la flèche droite pour passer à l'écran suivant.

Direction des communications

Cet écran permet le choix de la direction de communication et de l'hôte qui initie la communication.



D'abord, dans la section **La règle s'applique aux communications réalisées avec :** sélectionnez l'hôte distant. Quatre choix sont possibles :

n'importe quel autre ordinateur	Tout ordinateur autre que votre Macintosh.
les ordinateurs de mon réseau local	Tout ordinateur sur le même réseau local que votre Macintosh.
les ordinateurs d'un réseau AirPort standard	Tout ordinateur sur votre réseau AirPort par défaut, le cas échéant.
les ordinateurs du réseau sélectionné dans cette liste :	Si vous avez créé des réseaux personnalisés à l'aide de l'éditeur de règle standard, vous pouvez en sélectionner un dans ce cadre.

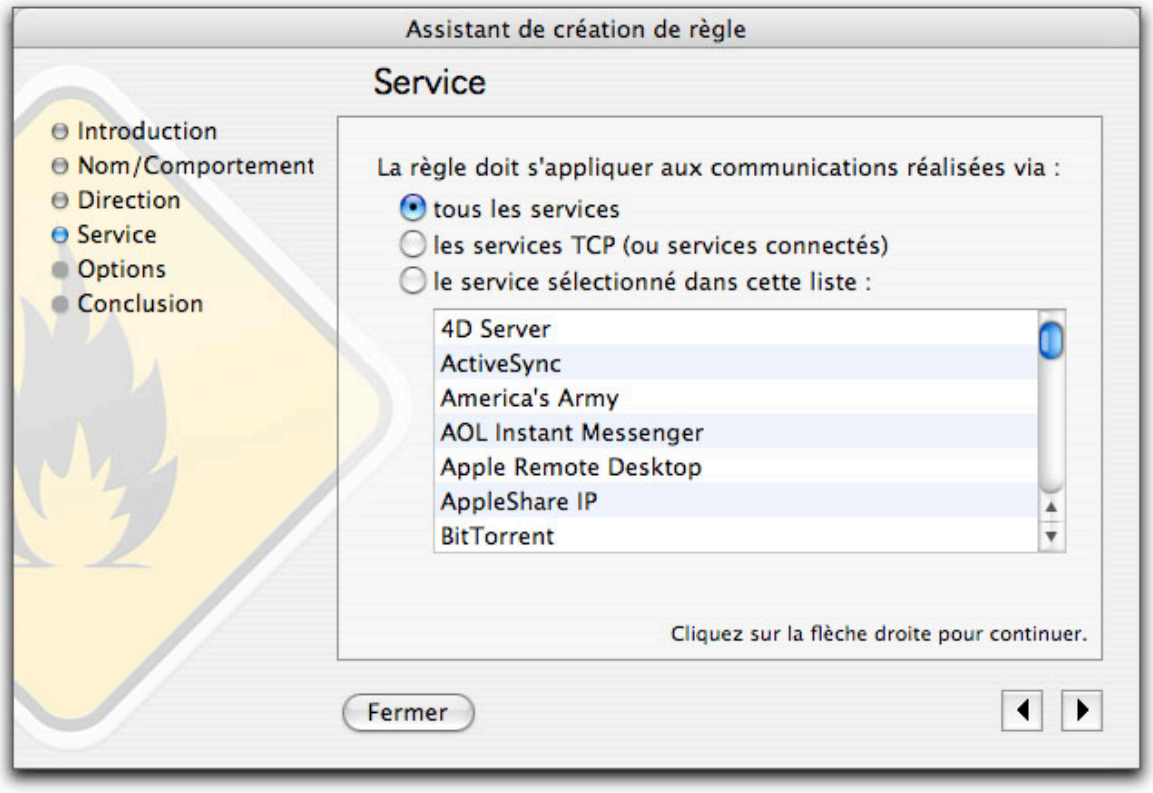
Puis, sélectionnez l'ordinateur qui initie la connexion :

Mon Mac	Votre ordinateur Macintosh, l'ordinateur utilisant cette règle.
l'autre ordinateur	L'ordinateur distant, défini dans la première partie de l'écran.

Quand c'est terminé, cliquez sur la flèche droite pour passer à l'étape suivante.

Service

Cet écran permet le choix du service auquel la règle va s'appliquer.



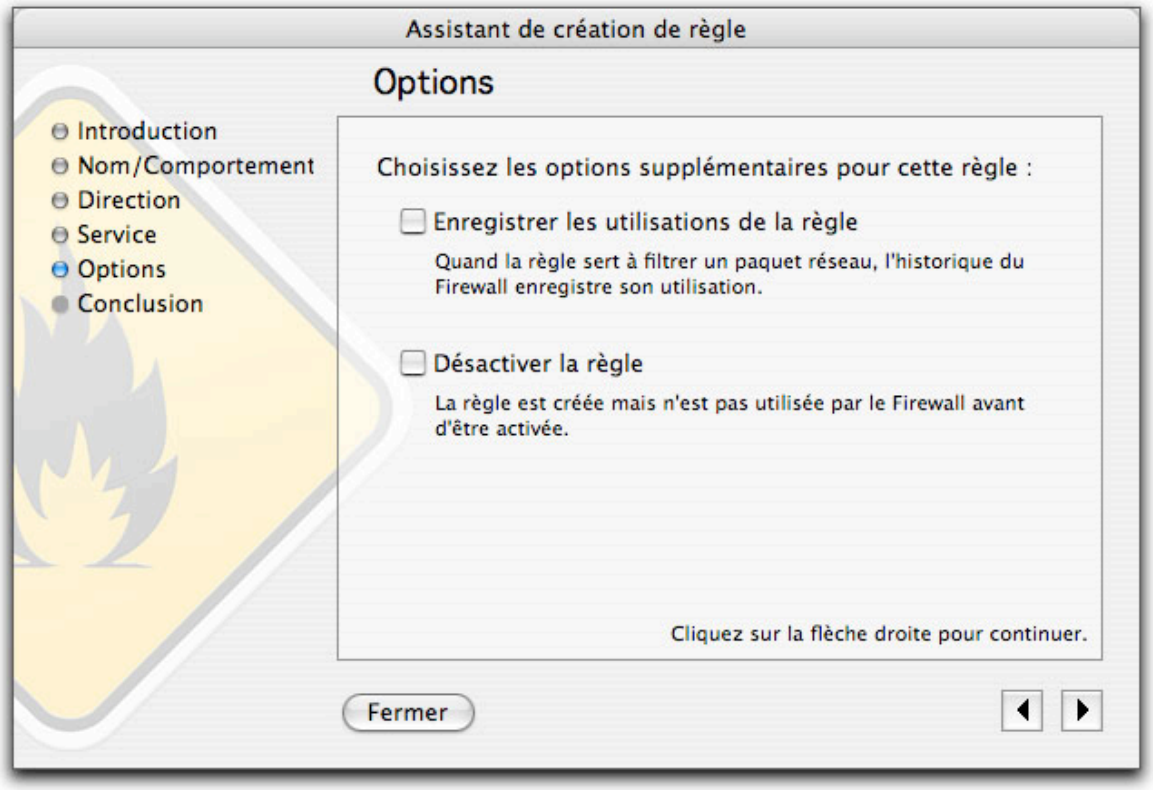
Trois types de services sont disponibles :

tous les services	Tous les services de réseau.
les services TCP (ou services connectés)	Services nécessitant une connexion ouverte et maintenue entre deux ordinateurs, tels que HTTP, FTP, TELNET, SSH, POP3, AppleShare, etc. Cela concerne toutes les connexions TCP.
le service sélectionné dans cette liste :	Vous avez le choix parmi la liste des services correspondant aux applications et protocoles les plus courants. Pour activer le service, sélectionnez-le en cliquant sur son nom.

Quand c'est terminé, cliquez sur la flèche droite pour passer à l'étape suivante.

Options

Cet écran permet le choix d'options de règle supplémentaires.



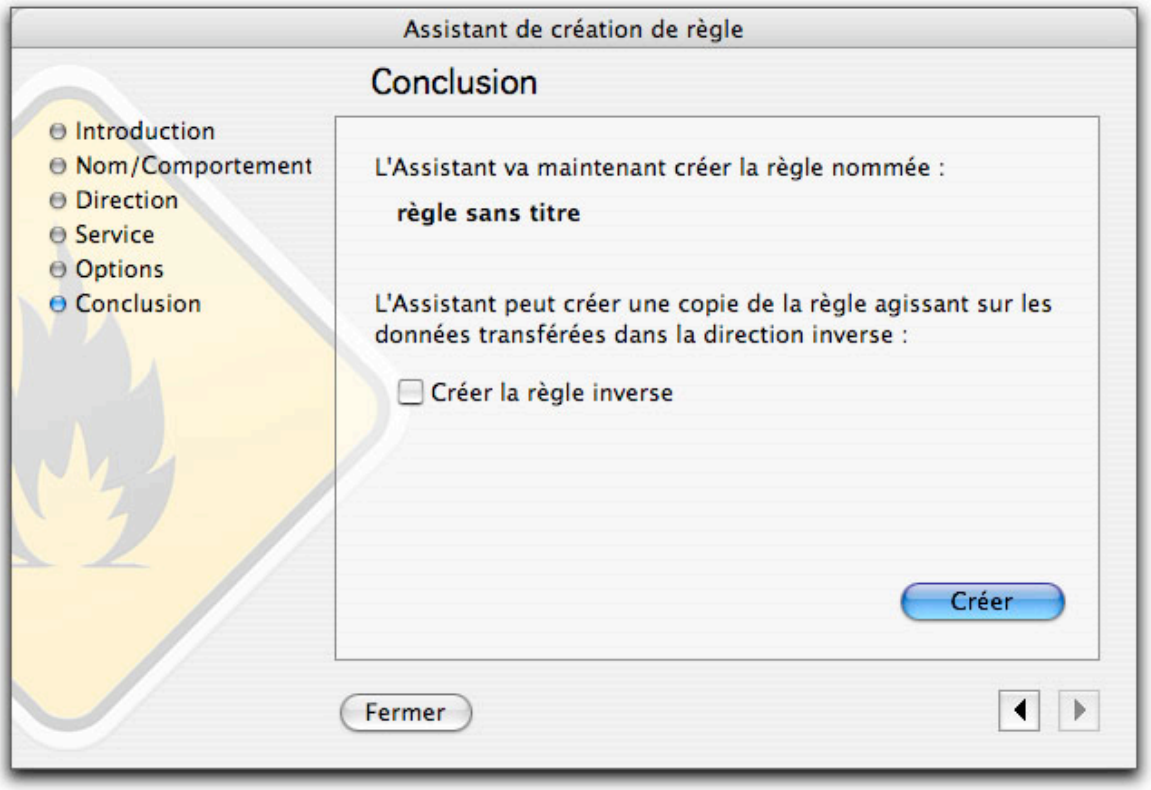
Deux options sont possibles :

Enregistrer les utilisations de la règle	Le firewall enregistre chaque utilisation de la règle dans l'historique.
Désactiver la règle	NetBarrier X5 crée la règle, mais la désactive. Vous pouvez l'activer manuellement au besoin.

Quand c'est terminé, cliquez sur la flèche droite pour passer à l'étape suivante.

Conclusion

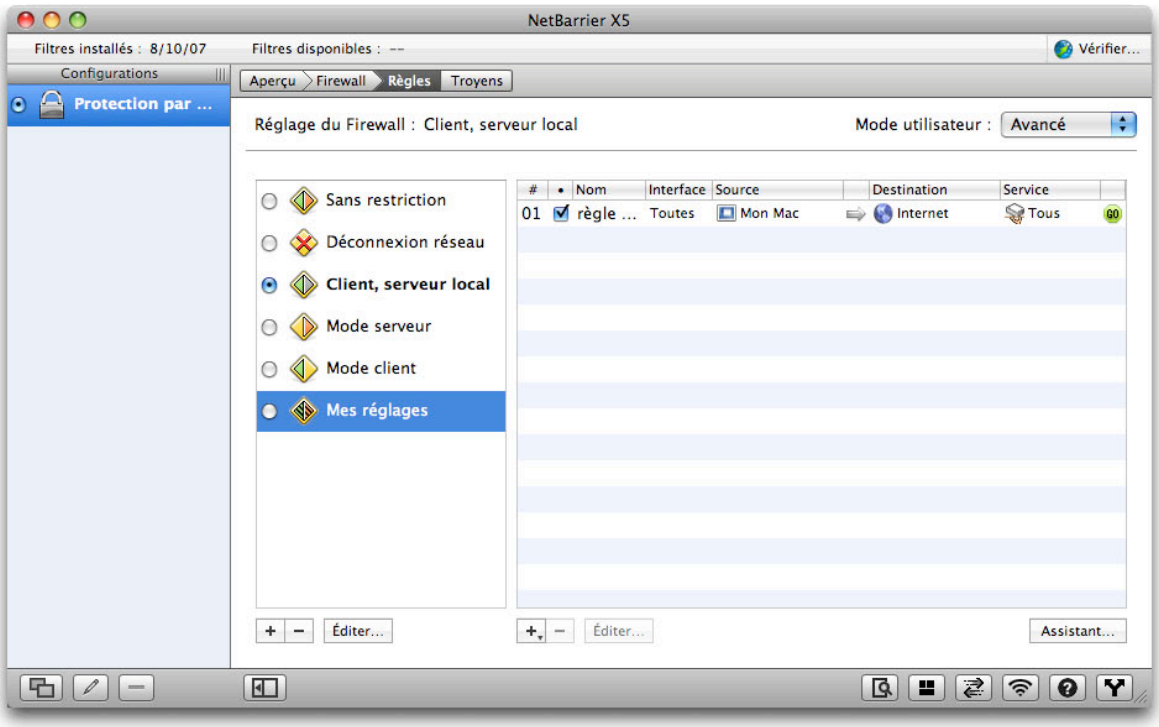
Cet écran permet la création de la règle selon les réglages effectués dans l'assistant.



Cet écran offre une option finale : si vous cochez **Créer la règle inverse**, l'assistant crée la règle correspondante, dont la source et la destination sont permutées.

Cliquez sur Créer pour créer la règle et quitter l'assistant de création.

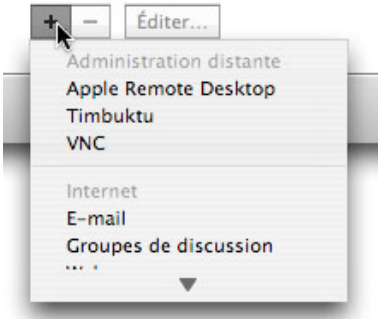
Quand c'est terminé, vous constatez que la règle (ou les règles, si vous avez coché **Créer la règle inverse**) apparaît dans la liste des règles de firewall de NetBarrier X5.



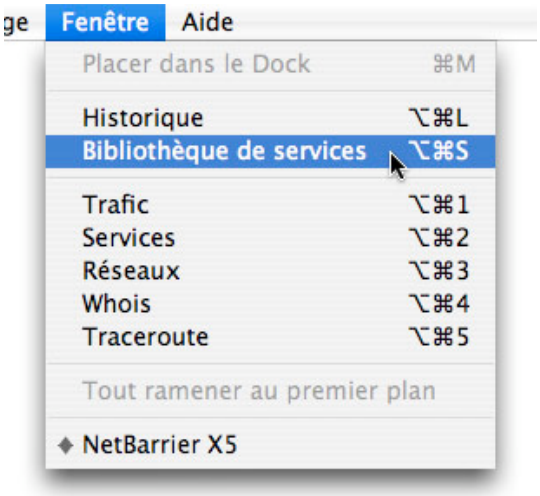
Pour une personnalisation plus poussée, ou des modifications, voir ci-dessous, **Mise en œuvre des règles**.

Création rapide de règles spécifiques à des services

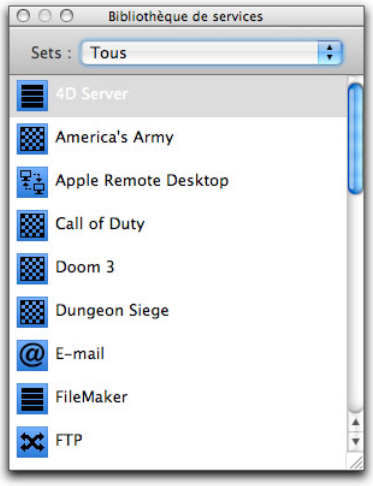
Il existe deux façons de créer rapidement des règles pour contrôler les informations allant et venant des services et des programmes courants. La première façon est de cliquer sur le bouton + au bas de la liste des règles et de maintenir le bouton de la souris enfoncé pendant une seconde. Vous pouvez alors choisir dans la liste déroulante parmi les services les plus courants. Une règle gouvernant votre sélection apparaît ensuite dans la liste des règles.



Le deuxième mode de création rapide passe par la Bibliothèque de services. Pour afficher cette bibliothèque, choisissez Fenêtre > Bibliothèque de services, ou tapez Option-Commande-S.



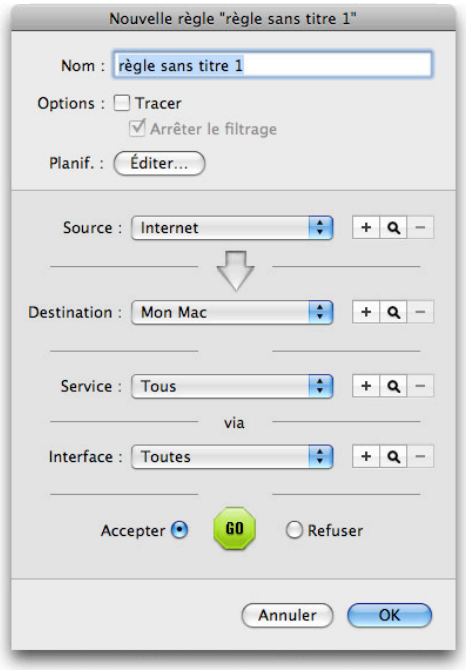
La fenêtre de la Bibliothèque de services s'ouvre et présente la liste des services les plus courants.



Pour créer une nouvelle règle, sélectionnez le service voulu et faites-le glisser vers la liste de règles. Par défaut, une règle ajoutée de cette façon autorise tout le trafic de votre Mac vers Internet, sur toutes les interfaces. En d'autres termes, la règle n'interdit aucune activité jusqu'à la modification éventuelle de ses éléments, comme décrit ci-après.

Création manuelle de règles

Vous pouvez créer des règles individuelles via l'éditeur de règle. Cliquez sur le bouton + au bas de la liste des règles et l'éditeur de règle apparaît.

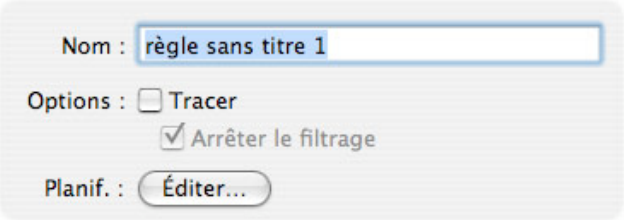


L'éditeur de règle de NetBarrier X5 permet aux administrateurs de réseau de procéder efficacement à la définition et la mise en œuvre d'une stratégie globale de sécurité. Il est extrêmement flexible et permet de créer un nombre illimité de règles. Une règle est définie en six éléments :

- **Nom de la règle, historique et planification**
- **Source de la règle**
- **Destination de la règle**
- **Service de la règle**
- **Interface**
- **Action de la règle**

Nom de la règle, historique, traçage et planification

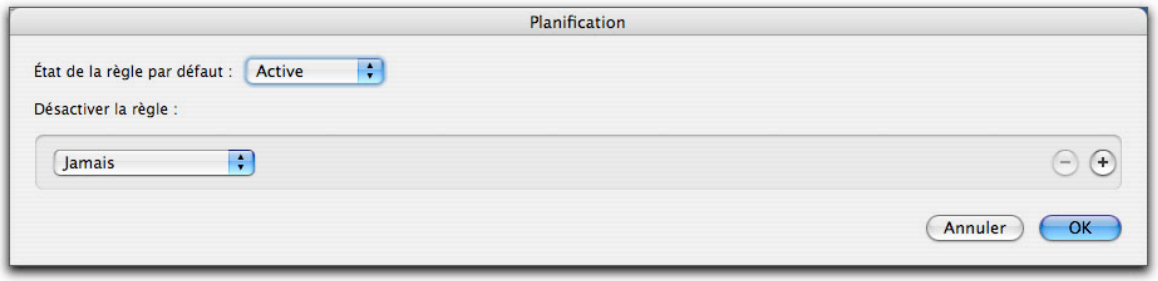
Le champ en haut de l'Éditeur de règle est destiné au nom de la règle. Juste en dessous se trouve la case **Tracer**. Si vous cochez la case **Tracer**, une entrée s'ajoute à l'historique de NetBarrier X5 à chaque action de cette règle ; un petit point rouge à droite du nom de la règle, dans la liste des règles, indique le traçage. Sinon, l'historique n'est pas conservé.



Si la case **Tracer** est cochée, la case **Arrêter le filtrage** devient disponible, et elle est cochée par défaut. Ces deux réglages, en tandem, constituent un outil performant de recherche de pannes sur un réseau sans gêner son trafic.

ATTENTION : Si vous ne comprenez pas pourquoi certaines règles n'ont pas d'effet, vérifiez les règles les précédant, et assurez-vous que la case "Arrêter le filtrage" soit désactivée pour chacune d'entre elles.

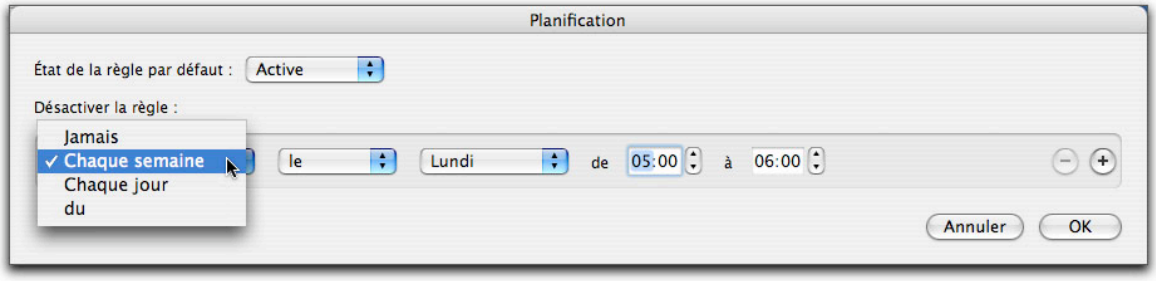
Pour modifier la planification, cliquez sur le bouton Editer... La fenêtre Planification apparaît :



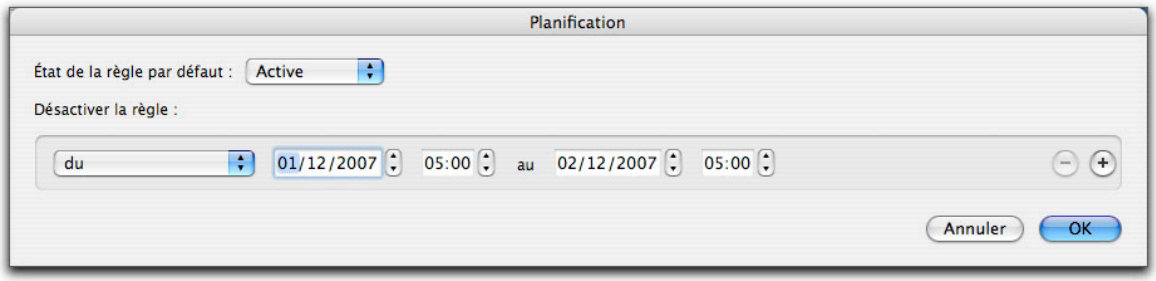
L'état de la règle par défaut est fixé à Active, ce qui signifie que la règle est activée. Si vous le réglez à Inactive, NetBarrier X5 n'utilise pas cette règle. Vous pouvez décider que certaines règles soient actives dans une configuration, et pas dans une autre. Pour en savoir plus sur l'utilisation des sets de configurations, reportez-vous au chapitre 10, **Préférences et configurations.**

Si l'état de la règle par défaut est Active, il est possible de régler des périodes spécifiques pendant lesquelles la règle est désactivée. De même, si l'état de la règle par défaut est Inactive, il est possible de régler des périodes spécifiques pendant lesquelles la règle est activée.

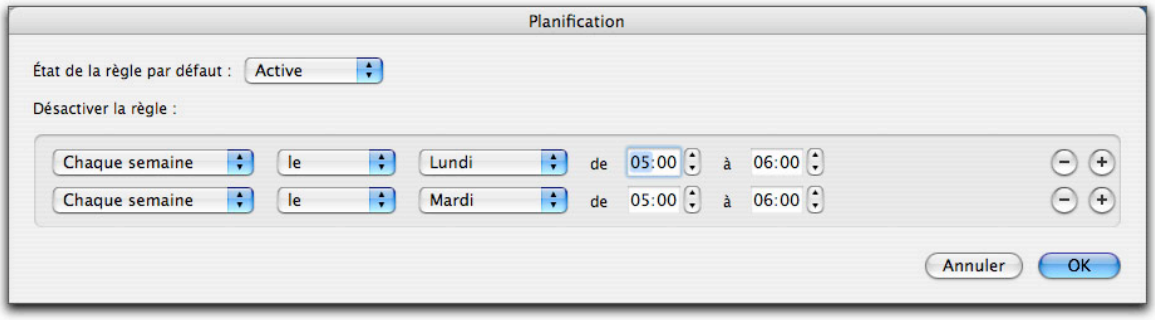
A la première création de règle, l'état de la règle par défaut est fixé à Active, et le menu Désactiver la règle est fixé à Jamais. En d'autres termes, si vous n'apportez pas d'autres modifications, la règle sera toujours active. Si vous souhaitez que l'état de la règle soit modifié à certains moments, cliquez sur le menu déroulant et sélectionnez un des intervalles de temps dans la liste.



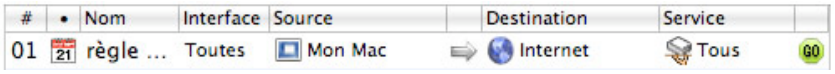
Trois options sont disponibles, en plus de Jamais. Chaque semaine et Chaque jour permettent de spécifier la modification de façon récurrente, hebdomadaire ou quotidienne, à des moments fixés, ou seulement certains jours de la semaine. En choisissant Du dans le menu déroulant, vous pouvez préciser une plage plus spécifique de modification. Dans le champ "Du", précisez la date et l'heure de début de la modification. Dans le champ "au", précisez la date et l'heure d'expiration de la modification.



A l'aide du bouton +, vous pouvez planifier d'autres périodes de modification de l'état de la règle. Par exemple, si la règle doit être désactivée les lundis et les mardis, vous pouvez régler ces deux jours dans la fenêtre Planification. Pour supprimer une période planifiée, cliquez sur le bouton – sur la ligne concernée.

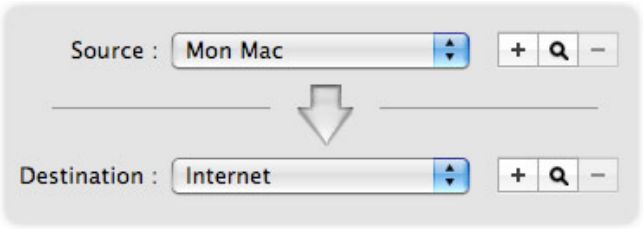


Les règles planifiées apparaissent avec une icône de calendrier dans la liste des règles. L'historique de cette règle particulière est activé, comme l'indique le petit point rouge à côté du nom.

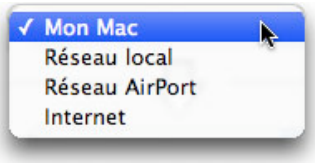


Source et destination de la règle

Dans la définition des règles, la source est l'entité qui envoie les données, et la destination l'entité qui les reçoie. Quatre sources et destinations sont disponibles pour chaque règle. Cependant, NetBarrier X5 ne permet pas de choisir la même entité comme source et destination dans une règle.



Les quatre sources et destinations disponibles par défaut sont les suivantes :



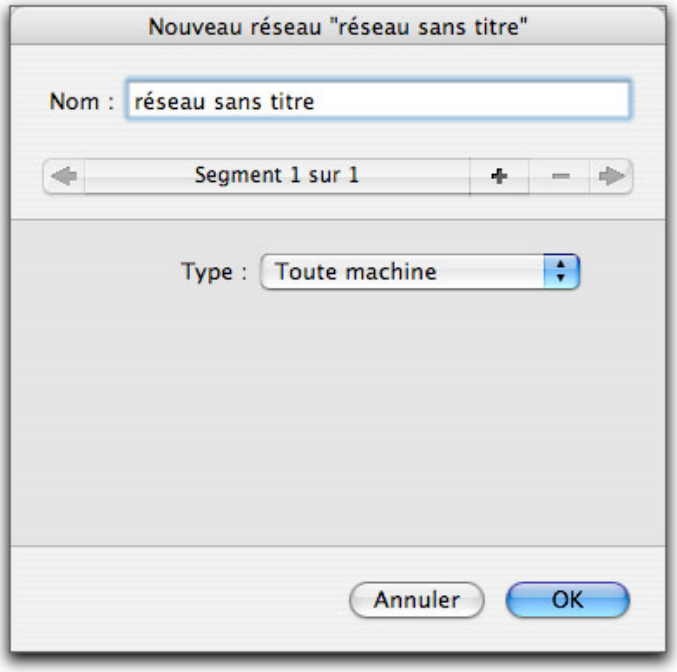
Mon Macintosh	Votre ordinateur.
Réseau local	Le réseau local auquel l'ordinateur est connecté.
Réseau AirPort	Le réseau AirPort sans fil auquel l'ordinateur est connecté.
Internet	L'Internet, en plus du réseau local auquel vous pouvez être connecté ; en fait, tous les réseaux.

Création de nouvelles sources et destinations

Vous pouvez créer de nouvelles sources et destinations à inclure dans les règles. Cela permet de spécifier les ordinateurs qui peuvent communiquer avec votre Mac.

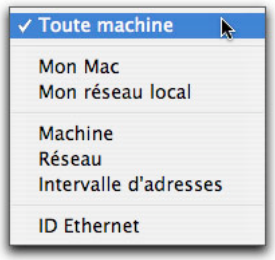
Pour créer une nouvelle source ou destination, cliquez sur le bouton + à droite du menu déroulant correspondant. Dans notre exemple, nous allons créer une nouvelle Source ; cependant, dès qu'elle est créée, elle va apparaître dans la liste des Destinations possibles.

L'éditeur de nouveau réseau apparaît.



Entrez un nom qui vous aidera à mémoriser le réseau. Si, par exemple, vous bloquez les adresses IP dont le dernier octet se situe dans l'intervalle 100-155, la Source/Destination pourrait s'appeler "IP de 100 à 155".

Le menu déroulant Type propose sept types de réseau.

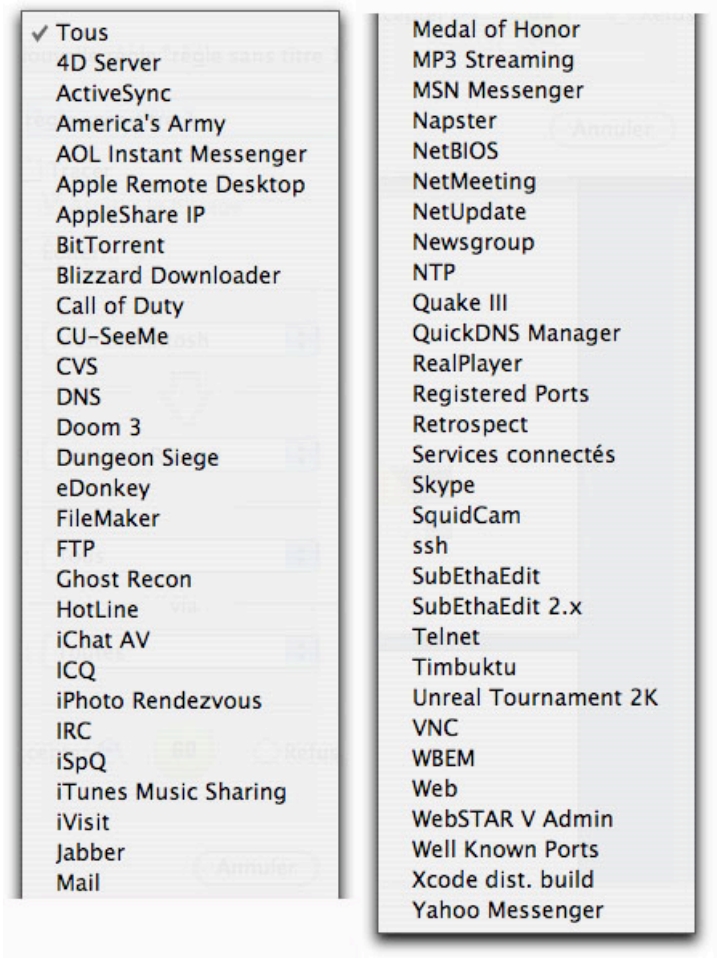


Nom	Définition	Type d'adresse
Toute machine	N'importe quel réseau.	Aucun, vu que cette adresse couvre tous les réseaux.
Mon Mac	Votre ordinateur.	L'(les) adresse(s) IP de votre Mac s'affiche(ent) dans le champ Adresse, non modifiable.
Mon réseau local	Le réseau local auquel l'ordinateur est connecté.	L'(les) adresse(s) IP de votre Mac et le masque subnet de votre réseau local s'affichent dans le champ Adresse, non modifiable.
Machine	Une adresse IP spécifique.	N'importe quelle adresse IP. Si vous entrez un nom de domaine, NetBarrier X5 le résout en une seule adresse IP.
Réseau	Un réseau spécifique.	N'importe quelle adresse IP Subnet et masque Subnet. Comme ci-dessus, NetBarrier X5 résout les noms de domaine en une seule adresse IP.
Intervalle d'adresses	Un groupe d'adresses IP.	Adresses initiale et finale. NetBarrier X5 résout les noms de domaine en une seule adresse IP.
ID Ethernet	Un seul élément connecté au réseau par Ethernet.	Une ID Ethernet, sous la forme de six nombres hexadécimaux à deux caractères.

Services de la règle

Le terme "Service" fait référence à la combinaison d'un type de protocole, du ou des ports utilisés, et de critères spécifiques au protocole. Ces éléments, pris ensemble, décrivent habituellement un programme, ou une classe de programmes, qui envoie et reçoit des informations. Par exemple, dans le cas d'informations envoyées par le protocole TCP sur le port 80 à l'aide de HTTP, il s'agit d'un service web.

NetBarrier X5 dispose d'une soixantaine de services courants, préprogrammés pour qu'il soit facile de bloquer (ou d'autoriser) le trafic qui relève d'un type spécifique.



Alors que la plupart des Services préprogrammés sont clairement mappés vers un programme spécifique, certaines sélections dans cette liste, telles que “Web” relèvent plutôt d'une classe de communications. Voici quelques exemples de services non spécifiques :

Nom	Description	Réglages
Tous	Toutes les communications, quel que soit le protocole ou le port.	Tous les protocoles, sur tous les ports.
Apple Remote Desktop	Programme permettant qu'un administrateur Mac contrôle un autre Mac via une connexion réseau.	Port 3283 sur UDP.
FTP	File Transfer Protocol.	TCP, ports 20 ou 21.
iChat AV	Programme de messagerie instantanée avec vidéo et son.	Port 5060 sur UDP.
IRC	Internet Relay Chat.	TCP sur port 194 pour IRC, et tou le trafic TCP entre les ports 6665 et 6669, inclus.
iTunes Music Sharing	Mode de partage de votre bibliothèque de musique sur iTunes via votre réseau local.	Port 3689 sur TCP.
Mail	Communications de courrier électronique.	TCP port 25 pour SMTP, port 110 pour POP3, port 143 pour IMAP4, port 220 pour IMAP3, port 389 pour LDAP, et port 587 pour le dépôt de messages.
NTP	Network Time Protocol.	UDP sur port 123.
Services connectés	Toutes les communications TCP. Une session TCP maintient une connexion entre ordinateurs ; il est donc bien clair qu'elle était initiée par le Mac et qu'elle est digne de confiance. Par comparaison, une session UDP est une série de communications sans la "mémoire" de l'initiateur.	Toutes les communications TCP, sur n'importe quel port.
SSH	Secure Shell.	TCP sur port 22 utilisant SSH.

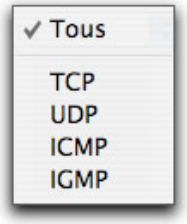
Telnet	Connexion à distance.	TCP sur port 23 utilisant telnet.
VNC	Virtual Network Computing, système graphique de contrôle à distance.	TCP sur ports 5900-5999.
Web	Navigation web, par exemple via un navigateur tel que Firefox.	TCP sur ports 80 et 8080 via HTTP, et sur port 443 via HTTPS.
Ports connus	Large intervalle de ports ayant une tradition de long usage en communications réseau.	TCP et UDP sur tous les ports de 0 à 1023.

Les autres services s'appliquent à des programmes ou protocoles spécifiques.

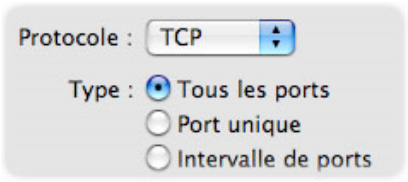
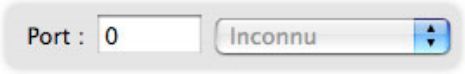
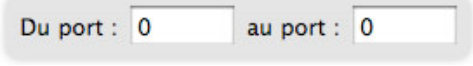
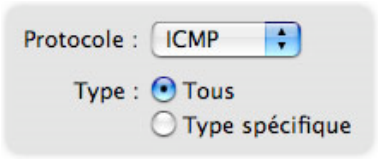
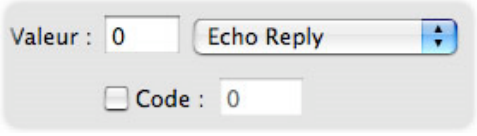
La création de règles pour des services spécifiques réclame la plus grande attention. Quand vous sélectionnez un service lié à un programme spécifique, il est possible que ce programme utilise le même port qu'un autre programme ou service. Le blocage ou l'autorisation d'un service spécifique risque de rentrer en conflit avec d'autres règles plus générales. Par exemple, si vous souhaitez bloquer le trafic ICQ, la sélection d'ICQ en tant que service bloquera également le trafic venant de AOL Instant Messenger, puisque ces deux programmes utilisent le même port. Il se peut que d'autres programmes utilisent les mêmes ports. Si vous avez des difficultés de connexion à un service donné, d'envoi ou de réception de données, essayez de désactiver les règles l'une après l'autre, jusqu'à dénicher le conflit.

Création de nouveaux services

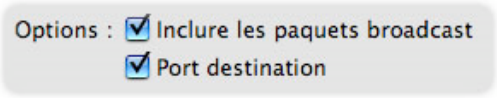
Vous avez le choix parmi quatre suites de protocoles dans le menu déroulant : TCP, UDP, ICMP et IGMP. Le choix de **Tous** couvre tous les protocoles.



Quand vous avez choisi une des suites de protocole, des options additionnelles apparaissent en partie basse du panneau, avec la liste des services disponibles. Les options dépendent du protocole. Pour plus d'informations sur ces protocoles et services, reportez-vous au chapitre 12, **Glossaire**.

Protocole	**Sélections de port**	**Options**
TCP ou UDP 	N'importe quel port	Pas d'option additionnelle
	Un seul port	 (Le menu déroulant propose plus de 100 options.)
	Intervalle de ports	
ICMP ou IGMP 	N'importe lequel	Pas d'option additionnelle
	Type spécifique	 (Le menu déroulant propose plus de 20 options.)

Pour chaque protocole, une option est disponible pour Inclure les paquets broadcast. Si cette option est cochée, les paquets envoyés à tous les ordinateurs sur un réseau local seront inclus dans ce service.

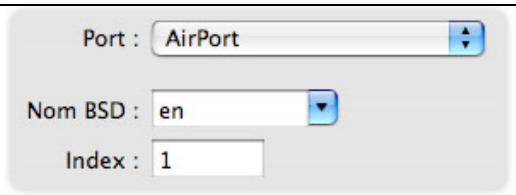
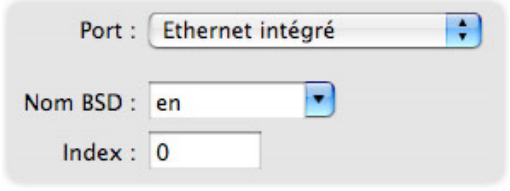
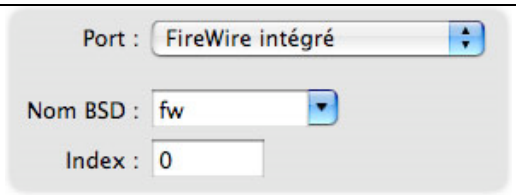


Le port destination est une option finale, disponible seulement pour les services utilisant le protocole UDP. Si l'option est cochée, les paquets sont filtrés selon la fonction du port de destination. Si elle n'est pas cochée, les paquets sont filtrés selon la fonction du port de source.

Interface de la règle

L'interface est l'adaptateur de réseau par lequel transitent les données. Il peut s'agir d'une carte Ethernet, une carte AirPort sans fil, une connexion PPP ou tout autre type d'interface réseau. Vous choisissez parmi une liste d'interfaces préprogrammées existant sur l'ordinateur, ou vous créez vos propres interfaces.

Le menu déroulant Type propose deux options. La première, Toutes, utilise toutes les interfaces de réseau disponibles. La seconde, Spécifique, liste les interfaces qui vous sont disponibles, selon le matériel et les logiciels de votre ordinateur. Les interfaces habituelles sont les suivantes :

AirPort Mise en réseau sans fil	
Ethernet intégré Interface câblée souvent utilisée pour la mise en réseau	
FireWire intégré Interface câblée souvent utilisée pour les périphériques	

Le nom BSD et le numéro d'index sont les identifiants utilisés par la couche Unix de Mac OS X. Si nécessaire, vous pouvez les régler manuellement. Si d'autres interfaces sont présentes sur votre Mac, une option Autre est également disponible.

Actions de la règle

Chaque règle a deux actions possibles : Accepter ou Refuser. Choisissez l'action souhaitée en cochant le bouton radio correspondant, en bas de la fenêtre de l'éditeur de règle.

Enfin, cliquez sur OK pour ajouter cette règle aux règles de Firewall de NetBarrier X5.

Sources, destinations, services ou interfaces en plusieurs segments

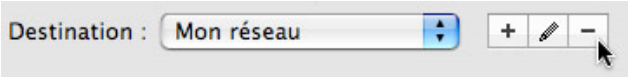
Les différents éléments d'une règle peuvent être définis en plusieurs segments. Vous pouvez, par exemple, décider que le trafic venant de plusieurs adresses IP spécifiques soit banni, en listant chacune séparément dans une source donnée.

Quand vous créez ou modifiez un élément (source, destination, service ou interface), une barre ayant l'aspect suivant apparaît en haut de la fenêtre :

Créer un nouveau segment	Cliquez sur le bouton +.
Se déplacer parmi les segments	Cliquez sur les icônes des flèches. Note : le texte au milieu indique le segment et le nombre total de segments. Quand vous avez atteint le dernier segment, cliquez sur la flèche droite pour revenir au premier.
Effacer un segment	Pour effacer un segment, il doit être visible. Cliquez sur l'une des icônes de flèche jusqu'à ce que le segment à effacer apparaisse. Cliquez sur le bouton –, puis confirmez l'effacement dans la boîte de dialogue qui suit.

Suppression de source, destination, service ou interface

Vous pouvez supprimer les éléments de règle créés. Choisissez l'élément concerné, puis cliquez sur le bouton .

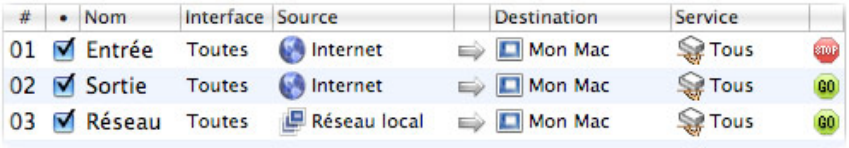


Une boîte de dialogue vous demande de confirmer la suppression. Sinon cliquez sur Annuler.

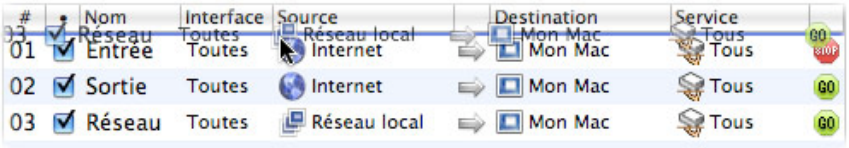
Mise en oeuvre des règles

Ordre des règles

Les règles que vous ajoutez au firewall de NetBarrier X5 sont activées dans l'ordre, de la première à la dernière ; vous devez vous assurer qu'elles sont classées dans un ordre logique, cohérent avec leur fonctionnement.



Ici, la première règle bloque les données venant d'Internet (ce qui inclut tous les réseaux, même un réseau local), tandis que la règle 3 permet le trafic venant d'un réseau local. Cependant, comme cette dernière est en troisième position, elle ne s'appliquera pas. Pour que la règle 3 s'applique, il faut la placer en tête de la liste des règles. Pour cela, sélectionnez la règle et faites-la glisser dans la position appropriée.



Modification et suppression de règles

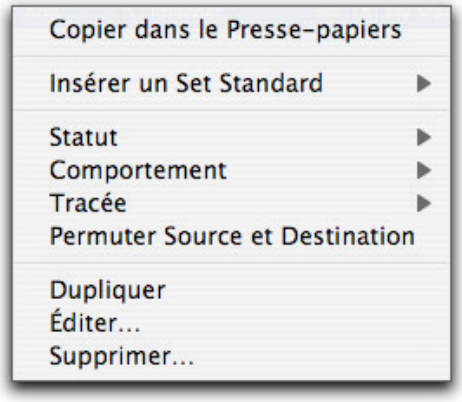
Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton portant un crayon au bas de la liste. L'éditeur de règle présente la règle, à modifier à votre convenance. Quand vous avez terminé, cliquez sur OK pour enregistrer les modifications. Sinon, cliquez sur Annuler.

Pour supprimer une règle, sélectionnez-la, puis cliquez sur le bouton - au bas de la liste.

Menu contextuel des règles

NetBarrier X5 permet d'apporter des modifications aux règles du firewall via un menu contextuel. Vous pouvez ainsi ajouter de nouvelles règles, modifier les règles existantes, ou modifier les caractéristiques d'une règle à la volée.

Vous accédez au menu contextuel en maintenant la touche Ctrl enfoncée et en cliquant sur une règle. (Avec une souris à deux boutons, il suffit de cliquer sur le bouton droit).



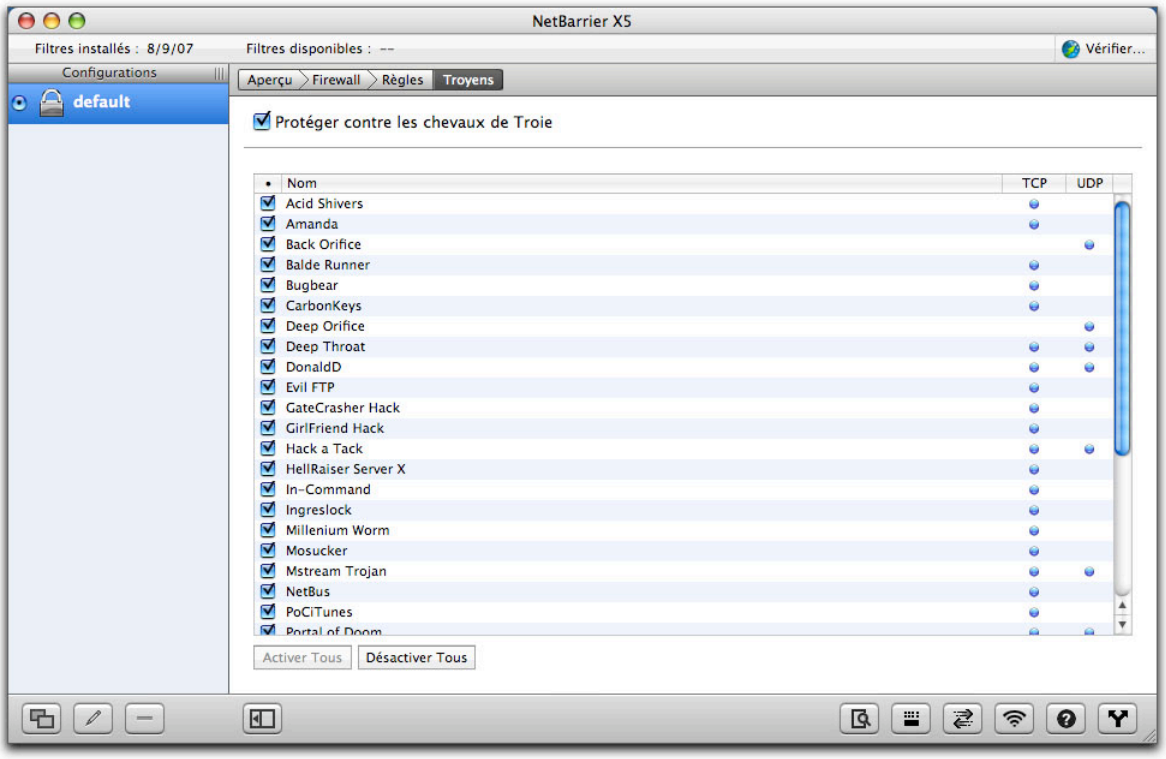
Le menu propose les options suivantes :

Copier dans le Presse-papiers	Pour copier le contenu d'une règle sur le presse-papiers du Mac au format texte seul. Vous pouvez ensuite coller la règle dans un document, où elle aura l'aspect suivant : "#02/ON/Input/Any/Internet -> My Mac/All/Deny" (où les barres obliques sont des tabulations).
Insérer un Set Standard / Ajouter un Set Standard	Pour insérer ou ajouter un set standard de règles, venant de la même sélection que celle trouvée en mode simplifié : Sans restriction, Déconnexion réseau, Client, serveur local, Mode serveur, ou Mode client.
Statut	Pour choisir l'état de la règle, entre Oui et Non. Si le fonctionnement de la règle est planifié, l'étiquette Planifiée est cochée dans le sous-menu.
Comportement	Pour choisir le comportement de la règle, et décider d'Accepter ou de Refuser le trafic.

Tracée	Pour choisir, entre Oui et Non, si la règle enregistre les données du trafic dans l'historique.
Permuter Source et Destination	Pour "inverser" une règle, en permutant la source et la destination.
Dupliquer	Pour faire une copie de la règle.
Éditer…	Pour ouvrir l'éditeur de règle pour la règle indiquée.
Supprimer…	Pour supprimer la règle.

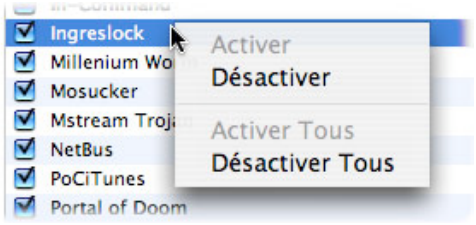
Protection contre les chevaux de Troie

Les chevaux de Troie sont des applications qui sont installées dans l'ordinateur subrepticement, soit par des pièces jointes truffées de virus et reçues avec des messages électroniques, soit par des programmes téléchargés ou achetés sur disque. Dans certains cas, les programmes installent un type particulier de cheval de Troie, appelé spyware, qui transmet des informations personnelles à un serveur. Comme la connexion se fait *depuis* votre ordinateur, elle est généralement traitée avec confiance. Cependant, NetBarrier X5 sait comment repérer les actions des chevaux de Troie les plus courants et les arrêter. Quelquefois, des programmes transmettent des informations relatives aux habitudes de navigation à un serveur central ; d'autres chevaux de Troie ouvrent des "portes dérobées" dans l'ordinateur, laissant ainsi la voie libre à la prise de contrôle par des pirates ou à la suppression de fichiers.



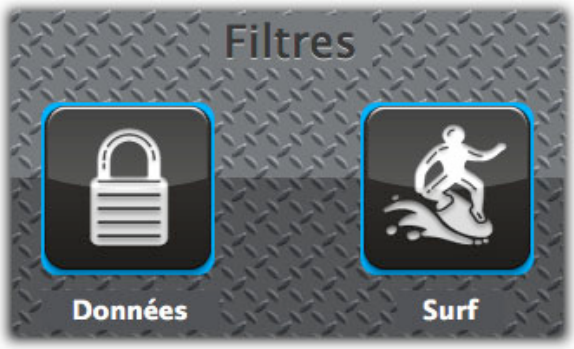
Pour activer la protection, cochez la case **Protéger contre les chevaux de Troie**, puis cliquez sur les noms des Troyens à sélectionner. Les boutons Activer Tous et Désactiver Tous, en bas de panneau, sont des raccourcis pratiques pour cocher ou décocher toutes les cases en une seule fois.

Vous pouvez également activer le blocage pour un seul cheval de Troie, ou pour tous les chevaux de Troie, en maintenant la touche Ctrl enfoncée et en cliquant sur le nom d'un Troyen. Un menu contextuel apparaît.



6 - Les Quatre lignes de défense : Filtres

Les filtres relatifs à la vie privée de NetBarrier X5 examinent toutes les paquets entrants et sortants à la recherche de types spécifiques de données. Il existe plusieurs filtres, séparés en deux sections : Données et Surf.

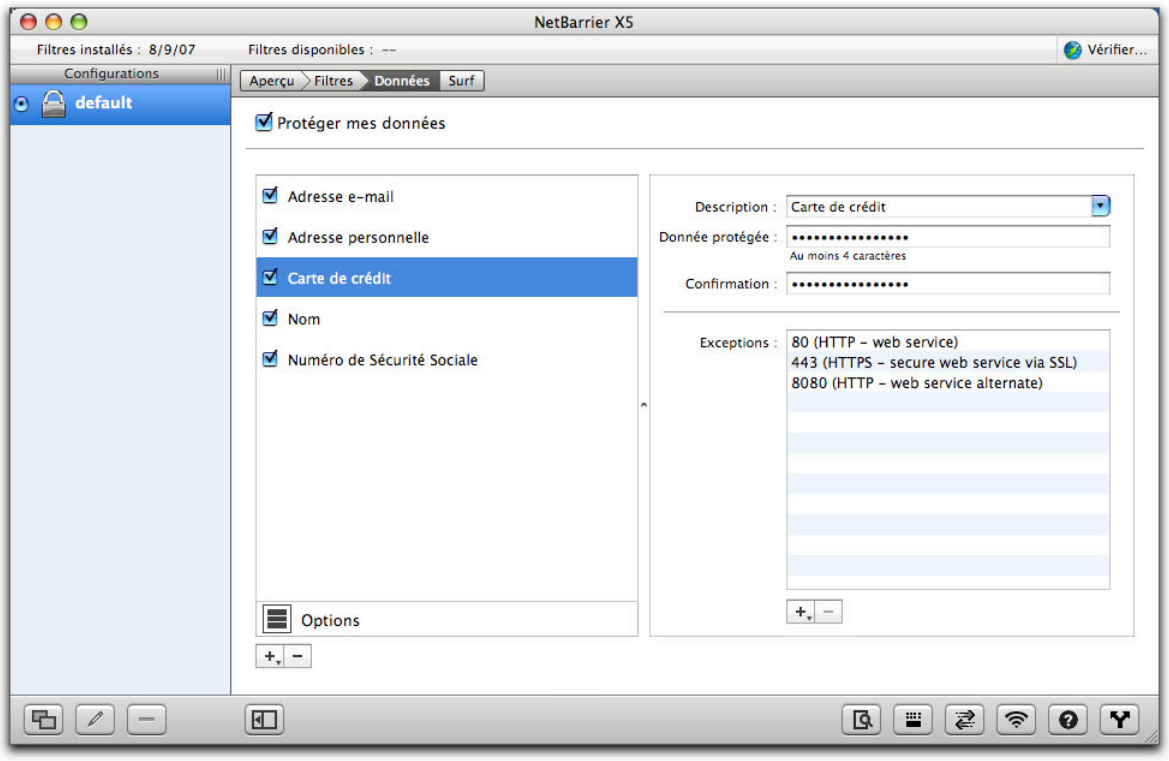


Filtre de données

Le filtre de données assure qu'aucune information sensible, que vous avez choisi de protéger, ne peut quitter votre Mac et partir sur un réseau. Vous déterminez précisément ce qui est à protéger ; par exemple, un numéro de carte de crédit, des mots de passe, ou des mots clés apparaissant dans des fichiers sensibles. Le filtre de données de NetBarrier X5 vérifie chaque paquet sortant pour s'assurer qu'aucun fichier contenant ces informations n'est transmis. Il protège non seulement contre l'envoi accidentel de fichiers contenant ces informations, mais également contre le risque de copie venant de quiconque disposant d'un accès réseau à votre Mac.

N'oubliez pas que, si votre ordinateur est accessible par réseau et si d'autres utilisateurs disposent de privilèges de partage de fichiers, ils peuvent copier vos fichiers.

Voici la fenêtre d'un filtre de données, avec quelques données en place :



Fonctionnement du filtre de données

NetBarrier X5 examine tous les paquets de données envoyés de votre ordinateur vers Internet ou un réseau local. Si l'une des données que vous avez indiquées dans le filtre est découverte, le paquet est bloqué.

Le filtre de données bloque seulement les données qui correspondent *exactement* au texte indiqué, y compris la ponctuation et la casse. Par exemple, si vous placez votre numéro de carte de crédit en donnée protégée, NetBarrier X5 empêche sa transmission depuis votre ordinateur et peut vous avertir de plusieurs manières, le cas échéant. Mais, si vous entrez le même numéro dans une page web sécurisée, il est crypté par votre navigateur. La donnée ne correspond plus exactement à la donnée protégée et elle peut être envoyée. Il en est de même pour les données qui sont codées selon d'autres manières, ou compressées.

Dans des cas extrêmement rares, le filtre arrête des données correspondant à vos critères mais pas à votre intention. Par exemple, les fichiers graphiques (tels que des images sur des sites web) se résument à des chaînes de données longues de milliers de caractères. Il est possible qu'un fichier graphique puisse, par simple coïncidence, contenir un élément de donnée que vous voulez protéger ; il serait donc bloqué par le filtre de données. (Si vous avez décidé de bloquer le nom “Jodie”, par exemple, un fichier graphique contenant la chaîne “Cg34gb$sEbOJodie8%” serait arrêté.) S'il vous arrive de ne pas pouvoir envoyer ou recevoir un élément spécifique d'information, essayez de désactiver le filtre de données momentanément, puis réactivez-le après le transfert.

Cochez la case **Protéger mes données** dans le coin supérieur gauche, pour activer le filtre de données. Vous pouvez le désactiver à tout moment, par exemple si vous voulez autoriser l'envoi ponctuel de données protégées.

Types de données à protéger

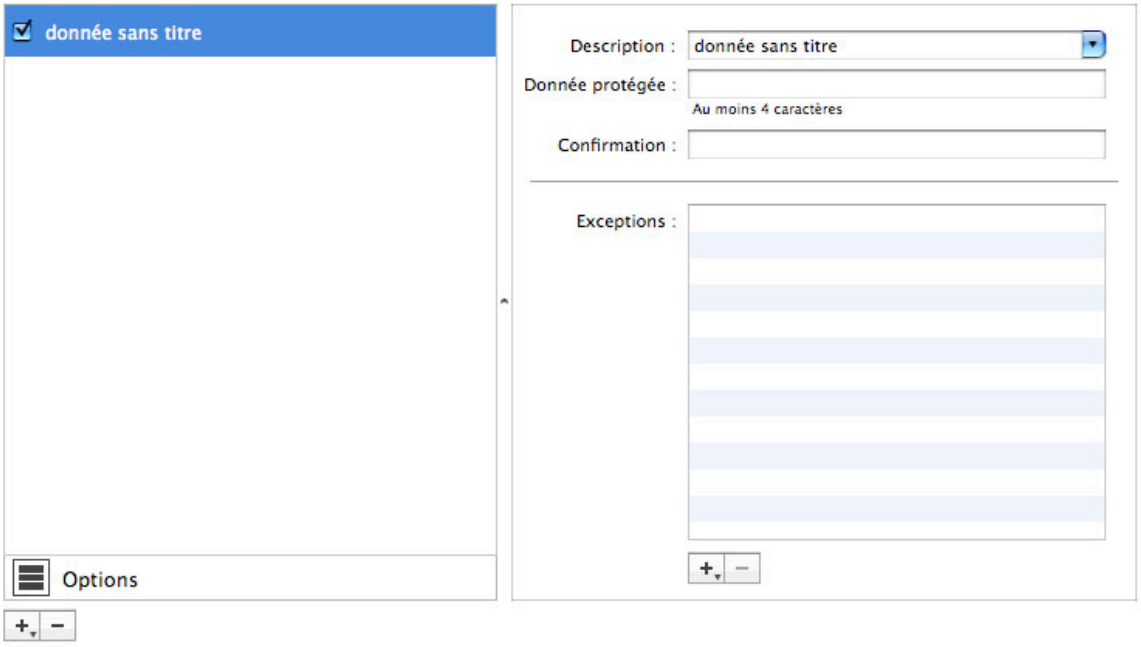
Le filtre de données inclut des étiquettes pour les cinq types les plus courants d'informations sensibles :

- **Carte de crédit**
- **Adresse e-mail**
- **Adresse personnelle**
- **Nom**
- **Numéro de sécurité sociale**

Cependant, ces étiquettes visent simplement la commodité. NetBarrier ne traite pas ces types différemment l'un de l'autre, ni de tous les types additionnels que vous pouvez décider d'ajouter - par exemple, "Numéro de téléphone", "Noms des enfants" ou "Mots de passe".

Ajout de données au filtre

Pour ajouter des données au filtre, cliquez sur le bouton + sous l'icône Options. Une nouvelle entrée appelée "donnée sans titre" apparaît dans la liste des filtres :

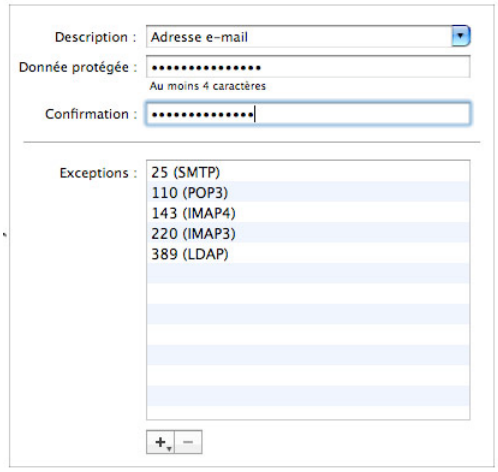


Entrez la description de la donnée protégée, dans le champ Description, ou choisissez-la dans le menu déroulant : vous constatez qu'elle est reprise par écho dans la liste des filtres. Puis entrez la donnée exacte à protéger dans le champ Donnée protégée. Ce texte est masqué pour qu'il reste invisible à quiconque jetant un coup d'oeil ou ayant accès ultérieurement à votre Mac. Vous devez entrer la même donnée une deuxième fois, dans le champ Confirmation. Si les champs Donnée protégée et Confirmation ne correspondent pas, un dialogue apparaît et donne le choix de rerégler la donnée protégée, auquel cas vous devez retaper les deux champs de données, ou de cliquer sur OK. Si vous cliquez sur OK, vous devez retaper la donnée protégée confirmée.

Pour que le filtre protège un texte, vous devez l'entrer *exactement* comme il se trouve dans vos documents. Par exemple, un numéro de carte de crédit peut apparaître comme XXXX-XXXX-XXXX-XXXX ou comme XXXX XXXX XXXX XXXX. Si vous protégez seulement le premier exemple, le filtre ne recherchera pas le second. De plus, cette donnée est sensible à la casse. Pour

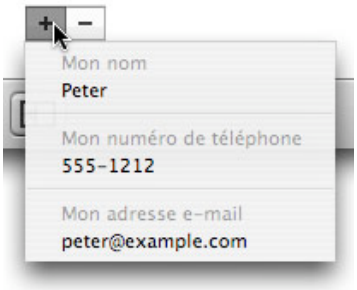
protéger un mot clé, tel qu'un nom de projet, vous devez indiquer toutes les casses possibles : Étude Marketing, étude marketing, ETUDE MARKETING, par ex.

La section **Exceptions** offre le choix de bloquer les données pour tous les services sauf ceux qui sont sélectionnés. Pour cela, cliquez sur le bouton +. Puis tapez le numéro de port du service. Alternativement, cliquez sur le signe + et maintenez le bouton de la souris enfoncé pendant quelques secondes : vous pouvez alors choisir dans la liste déroulante des services courants. (Certains, tels que Mail dans l'exemple ci-dessous, ajoutent plusieurs ports en une seule fois.) Vous pouvez ajouter un seul numéro de port, ou un intervalle de numéros de port, par exemple, 110-123. Les données vers ce port (ou ces ports) ne seront pas bloquées. Pour ajouter un autre service, répétez l'opération ci-dessus. Ajoutez autant de services que nécessaire.



Vous pouvez aussi glisser-déposer des services venant de la Bibliothèque des services. Cette option est particulièrement utile si vous ne connaissez pas les numéros de port spécifiques que vous souhaitez ajouter à la liste. Pour afficher cette bibliothèque, choisissez Fenêtre > Bibliothèque de services, ou tapez Option-Commande-S. Sélectionnez le service voulu, puis faites-le glisser vers la liste des Exceptions.

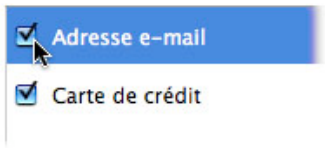
Vous pouvez ajouter certaines informations personnelles venant de votre fiche dans le Carnet d'adresses d'Apple, si vous en avez rempli une. Pour cela, cliquez et maintenez le bouton +, et trois éléments apparaissent : Mon nom, Mon numéro de téléphone et Mon adresse e-mail. Sélectionnez l'élément choisi pour l'ajouter en donnée protégée.



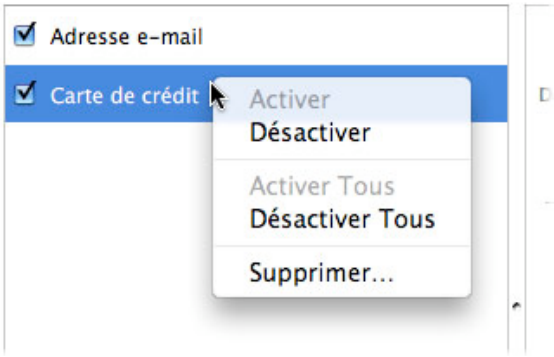
Dès que vous avez fini d'entrer ces informations, vos données sont protégées. Vous pouvez, à tout moment, revenir en arrière pour modifier un élément d'une donnée, en cliquant dessus dans la liste du filtre de données, et en modifiant les informations dans son panneau à droite.

Activation, désactivation et suppression des éléments de données$$

Chaque élément de donnée protégée est listé dans la fenêtre du filtre de données. La case à gauche de chaque ligne permet d'activer ou désactiver le filtrage de l'élément en question. Quand vous ajoutez un nouvel élément de donnée, la case est cochée par défaut. Si vous souhaitez envoyer cette donnée sur Internet ou sur un réseau local, vous devez décocher la case concernée, ou désactiver tous les filtres de données en décochant **Protéger mes données** comme indiqué plus haut.



Vous pouvez également activer ou désactiver le filtre de données pour des éléments individuels de données, ou pour l'ensemble des éléments, en maintenant la touche Ctrl enfoncée et en cliquant sur le nom d'un élément, ou en cliquant avec le bouton droit de la souris. Un menu contextuel apparaît.

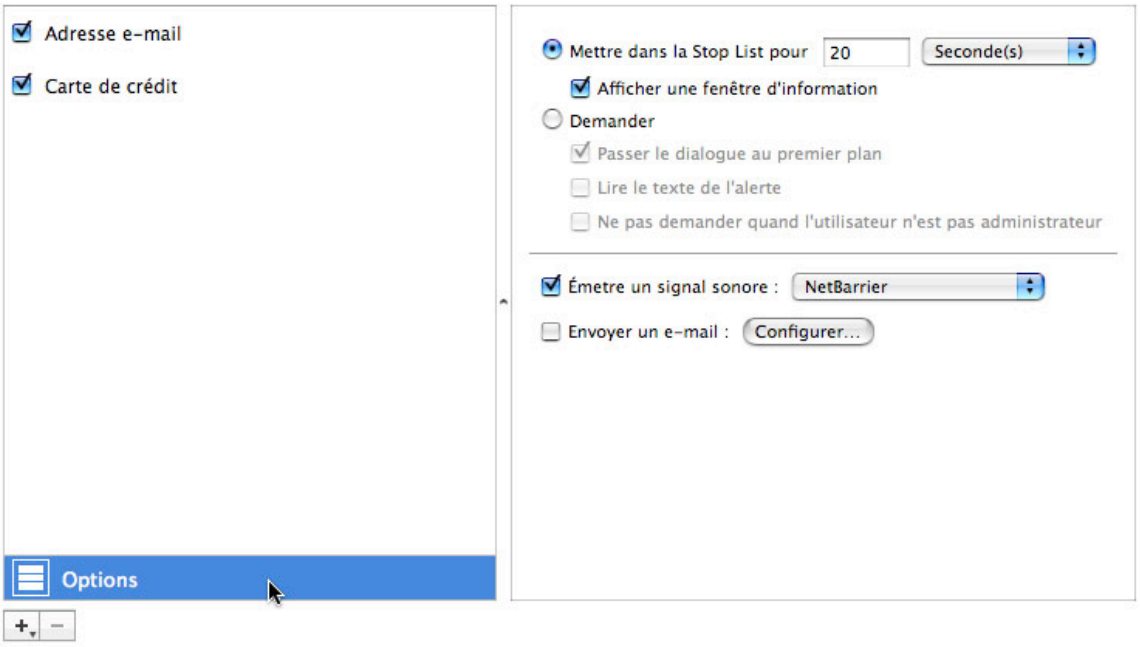


Sélectionnez Désactiver pour désactiver la protection de l'élément choisi, ou Désactiver tous pour désactiver la protection de tous les éléments. (Si l'élément choisi dans l'exemple ci-dessus était déjà désactivé, les choix pour Activer et Activer tous auraient été disponibles.)

Pour supprimer l'élément de façon permanente dans la liste du filtre de données, soit Ctrl-cliquez comme décrit ci-dessus et choisissez Supprimer..., soit sélectionnez l'élément de donnée et cliquez sur le bouton – . Dans chaque cas, une boîte de dialogue demande de confirmer la suppression.

Options du filtre de données

Quand une donnée protégée essaie de pénétrer ou de quitter votre Mac, vous disposez de plusieurs options sur le mode de notification et le mode de réaction aux tentatives futures. Pour voir les options, cliquez sur le bouton Options en bas à gauche du panneau. Les modifications des options affectent l'ensemble des données filtrées.



Pour en savoir plus sur les options, reportez-vous au chapitre 9, **Comprendre les alertes**.

Filtres de surf

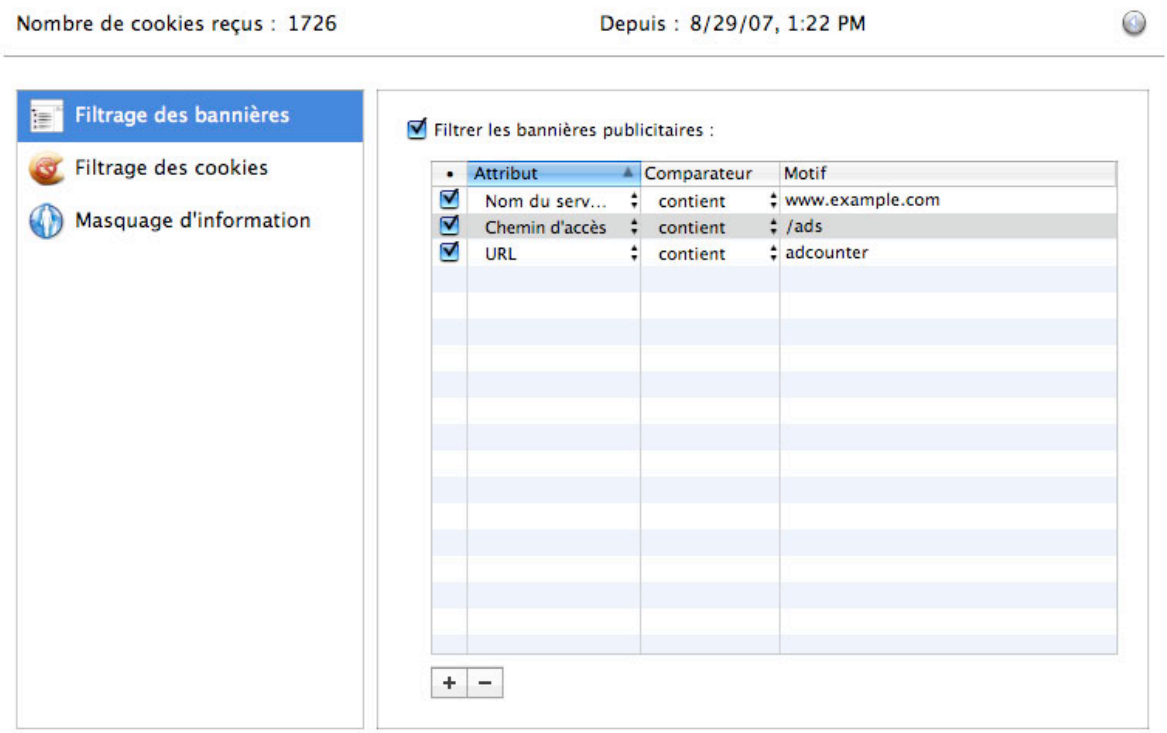
NetBarrier X5 inclut trois catégories de filtres pour aider à contrôler les informations échangées par votre Mac lors du surf sur Internet :

- Le **filtre des bannières** masque les bannières publicitaires sur les sites web visités ;
- Le **filtre des cookies** évite que votre Mac envoie certaines informations aux sites web qui suivent la trace de vos mouvements ;
- Le filtre de **masquage d'information** cache certains faits relatifs à votre Mac, votre navigateur web, le dernier site web visité et votre compte iTunes.

Les filtres de surf affectent tous les programmes de l'ordinateur qui communiquent via le protocole HTTP (consultez le chapitre 12, **Glossaire**). Les navigateurs web sont les programmes les plus courants utilisant HTTP, mais ce protocole concerne également iTunes, les lecteurs d'infos RSS, ainsi que de nombreux logiciels capables de naviguer sur Internet. En cas de difficultés inattendues avec ces programmes – lors du téléchargement de musique via iTunes, par exemple – essayez de désactiver temporairement les filtres de surf.

Filtrage des bannières

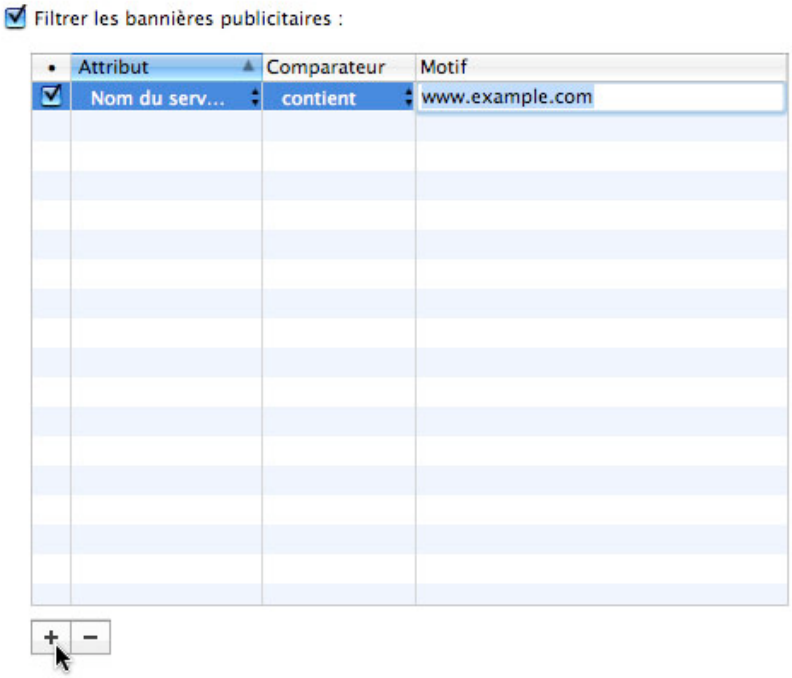
Le filtre de bannières est constitué d'une liste des règles utilisées par NetBarrier X5 pour filtrer des éléments indésirables sur le web, tels que les publicités graphiques appelées "bannières publicitaires", et aider à accélérer la navigation sans distractions superflues. NetBarrier X5 bloque ces publicités et les remplace par des petits graphiques transparents. NetBarrier X5 possède une liste de chaînes de bannières publicitaires à filtrer ; cependant vous pouvez ajouter des chaînes personnalisées, pour mieux filtrer les pubs rencontrées en surfant. Voici la fenêtre du filtre de bannières, avec quelques échantillons de données :



Pour activer le filtrage, cochez la case **Filtrer les bannières publicitaires**.

Ajout de règles au filtre de bannières

Le filtre contient déjà un jeu de règles, qui est tenu à jour lors de la mise à jour des Filtres de NetBarrier X5 à l'aide de NetUpdate X5. Il est facile d'ajouter vos propres règles ; pour cela, cliquez sur le bouton +. Une nouvelle ligne est ajoutée à la liste, il vous reste à la modifier.



La liste comporte quatre colonnes : une case à cocher, Attribut, Comparateur et Motif. Le motif précise le mode de définition de ce que vous voulez bloquer.

Le menu déroulant Attribut propose trois options :

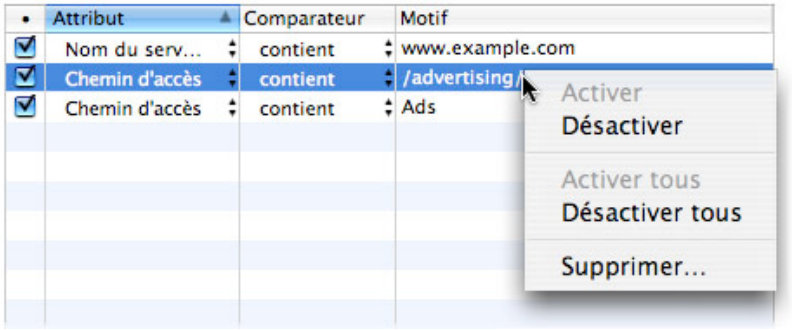
Nom du serveur	Le domaine Internet – c'est-à-dire, tout ce qui se trouve entre http:// et le premier "/" dans une adresse web. La valeur par défaut est www.example.com. Note : une telle entrée ne bloquerait pas (par exemple) http://forums.example.com ; pour bloquer les deux, il vaut mieux entrer example.com.
Chemin	Toute partie de l'URL suivant le nom du serveur ; par exemple, /ads/ dans http://www.example.com/home/graphics/ads/6542.html.
URL	L'URL en entier ; par exemple, http://www.example.com/home/graphics/ads/6542.html.

Le menu déroulant **Comparateur** permet le choix entre le blocage du contenu basé sur une correspondance exacte (“est”) ou partielle, quand votre texte correspond au moins à une portion de l'URL, (“contient”).

Activation ou désactivation des règles de bannières

Chaque règle de bannière apparaît sur une ligne dans la fenêtre des bannières. La case à cocher à gauche de chaque ligne permet d'activer ou désactiver le filtrage de la règle en question. Quand vous ajoutez une nouvelle règle, la case est cochée par défaut et le filtre est actif. Pour arrêter de bloquer certaines bannières, désactivez les cases concernées.

Vous pouvez également activer le blocage de bannières pour une règle individuelle de bannière, ou pour l’ensemble des règles, en maintenant la touche Ctrl enfoncée et en cliquant sur le nom d’une règle. Un menu contextuel apparaît.



Sélectionnez Désactiver pour désactiver la protection pour la règle choisie, ou Désactiver tous pour désactiver la protection pour toutes les règles. (Si la règle était déjà désactivée, les choix pour Activer et Activer tous auraient été disponibles.)

Pour supprimer une règle de bannière, soit choisissez l’option Supprimer… dans le menu contextuel, soit cliquez sur le bouton – sous la liste des règles.

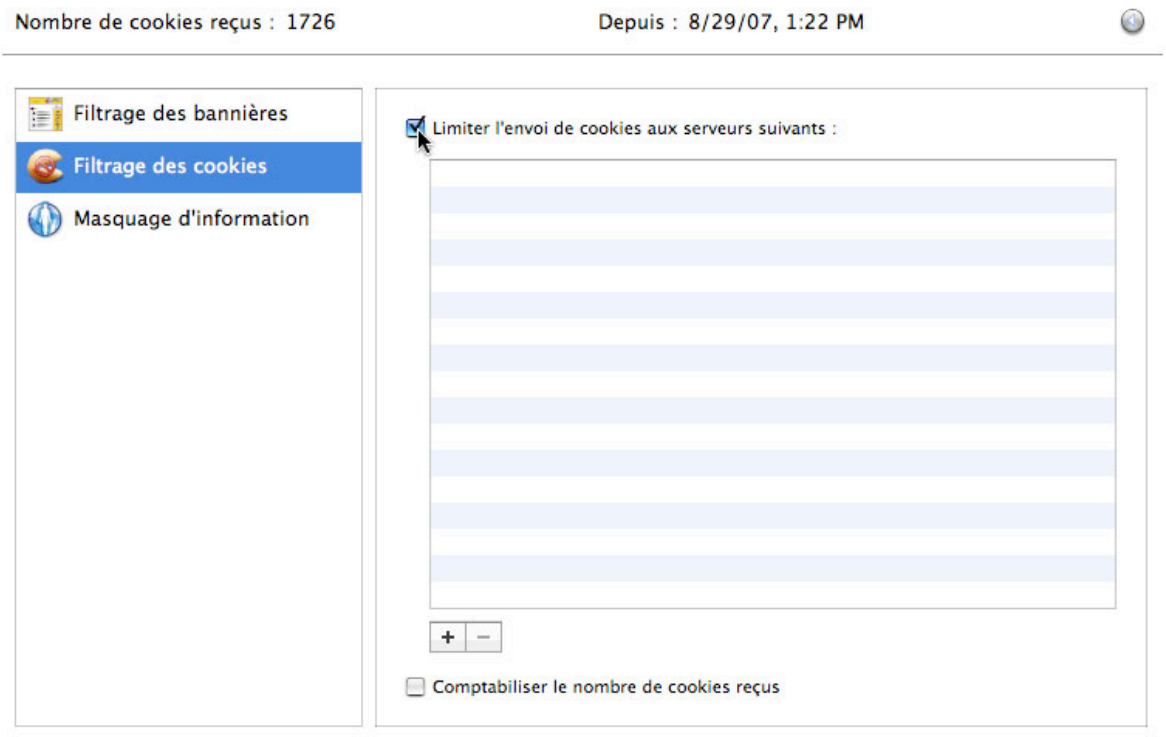
Note : le filtre de bannières ne reconnaît pas le contenu filtré, mais seulement la correspondance entre l'URL et les critères spécifiés. En conséquence, il se pourrait que vous ayez des difficultés occasionnelles pour consulter des informations sur les pages web qui coïncideraient avec vos critères, sans être réellement des bannières publicitaires. Si tel est le cas, essayez de désactiver temporairement le filtre de bannières. Vous pouvez le faire dans l'application NetBarrier X5, ou depuis le menu Intego, placé dans la barre de menus.

Filtrage des cookies

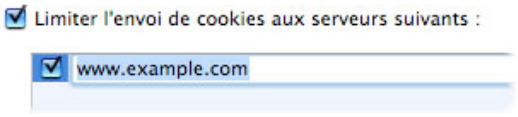
NetBarrier X5 inclut un filtre de cookies, qui évite que votre Mac envoie des informations de traçage, appelées "cookies", à tous les sites Internet, sauf à ceux que vous spécifiez.

Le filtrage de cookies est utile quand vous voulez surfer dans le plus strict respect de votre vie privée, en réservant à quelques sites dignes de confiance le suivi de vos actions. Cependant, de nombreux sites web – particulièrement ceux qui exigent un mot de passe – ne vont pas fonctionner correctement, à moins de les inclure dans la liste des sites de confiance.

Pour activer le filtrage, cochez la case **Limiter l'envoi de cookies aux serveurs suivants**.



Pour ajouter un serveur à la liste de filtrage des cookies, cliquez sur le bouton + au bas de la liste. Une fausse adresse de serveur (www.example.com) apparaît. Modifiez-la pour le site de votre choix.



Remplacez la fausse adresse par le nom du serveur auquel l'envoi de cookies est autorisé. Vous pouvez faire glisser un URL venant d'un navigateur, ou même un URL en format texte, vers ce champ pour l'ajouter à la liste.

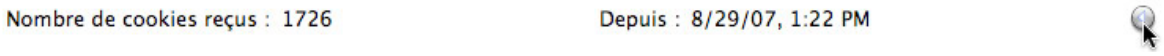
Comme pour le filtre de bannières, vous pouvez activer ou désactiver les filtres de cookies individuels en cochant les cases concernées, ou en maintenant la touche Ctrl enfoncée tout en cliquant sur le nom d'un élément et en utilisant le menu contextuel, ou en cliquant avec le bouton droit de la souris.

Pour supprimer les cookies déjà installés sur votre Mac, reportez-vous au manuel relatif à Intego Washing Machine, qui accompagne NetBarrier X5.

Compteur de cookies

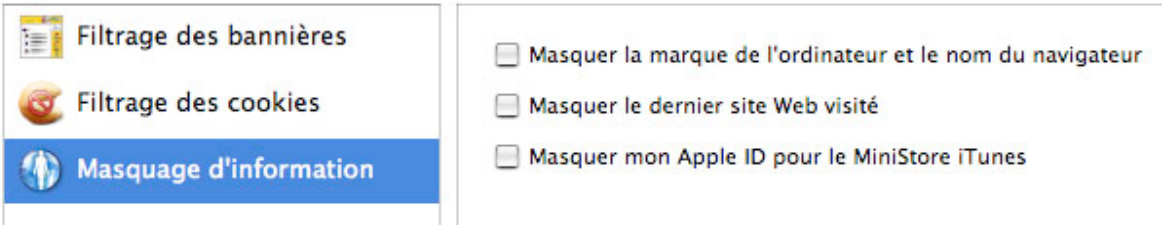
NetBarrier X5 peut compter le nombre de cookies envoyés à tous les utilisateurs de votre Mac, si vous cochez la case **Comptabiliser le nombre de cookies reçus**, au bas du panneau du filtre de cookies.

En haut du panneau est affiché le cumul du nombre de cookies acceptés par votre Mac depuis le dernier lancement ou la dernière remise à zéro du compteur. Vous pouvez, à tout moment, remettre le compteur à zéro en cliquant sur la petite flèche dans le coin supérieur droit.



Masquage d’informations

Tous les navigateurs sont réglés pour répondre aux demandes venant des sites web, à propos de la plate-forme (Mac, Windows, Linux, etc.) ainsi que du navigateur et de la version utilisés. Ces données peuvent aider le site à optimiser la livraison d'informations, par exemple, en activant des fonctionnalités adaptées au navigateur utilisé. Par ailleurs, certains sites limitent l'accès selon la plate-forme et le navigateur, allant même jusqu'à interdire l'accès aux utilisateurs de Macintosh. NetBarrier X5 sait masquer certaines données concernant votre ordinateur, ce qui pourrait autoriser l'accès, là où il serait refusé.



NetBarrier X5 peut répondre à ces demandes et n'envoyer que des données génériques. Par exemple, votre ordinateur va répondre au site web que vous utilisez un navigateur Netscape ou Mozilla, mais sans numéro de version ni plate-forme. Pour cela, cochez la case **Masquer la marque de l’ordinateur et le nom du navigateur**.

Certains sites gardent la trace du dernier site visité. Bien sûr, cela peut rendre votre navigation sur le web plus intéressante si, par exemple, un site commerçant offre des réductions quand vous venez d'un site web spécifique. Cependant, des sites peu scrupuleux pourraient utiliser cette fonctionnalité pour suivre vos habitudes de façon gênante. En cochant la case **Masquer le dernier site Web visité**, NetBarrier X5 évite que votre Mac ne réponde à ce type de demande.

Enfin, si vous utilisez iTunes et vous affichez le MiniStore iTunes, le logiciel transmet votre Apple ID aux serveurs d'Apple chaque fois que vous cliquez sur une chanson. Pour bloquer cela, cochez **Masquer mon Apple ID pour le MiniStore iTunes**. Cela n'empêche pas l'achat de musique sur le Store iTunes, mais cela évite l'envoi par iTunes d'informations liant votre navigation à votre compte sur le Store iTunes.

7 - Les Quatre lignes de défense : Antivandale

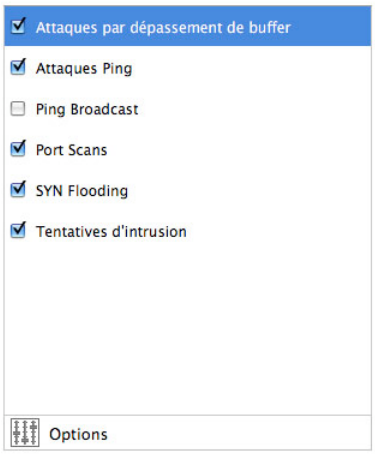
Antivandale

L'Antivandale de NetBarrier X5 surveille et filtre toutes les données entrant dans votre Mac, à la recherche de signes d'intrusion. Ce filtrage est transparent : NetBarrier X5 n'est visible qu'en cas de détection de données suspectes. Dans ce cas, une alerte apparaît. Sinon, l'Antivandale surveille l'activité réseau de l'ordinateur, en silence et en permanence.

La section Antivandale comporte deux fonctions contrôlant la façon dont les données pénètrent dans votre ordinateur : Politiques et Anti-Spyware. La Stop List et le Groupe de confiance stockent des hôtes spécifiques, ou des adresses IP, que vous jugez dignes de confiance ou pas.

Politiques

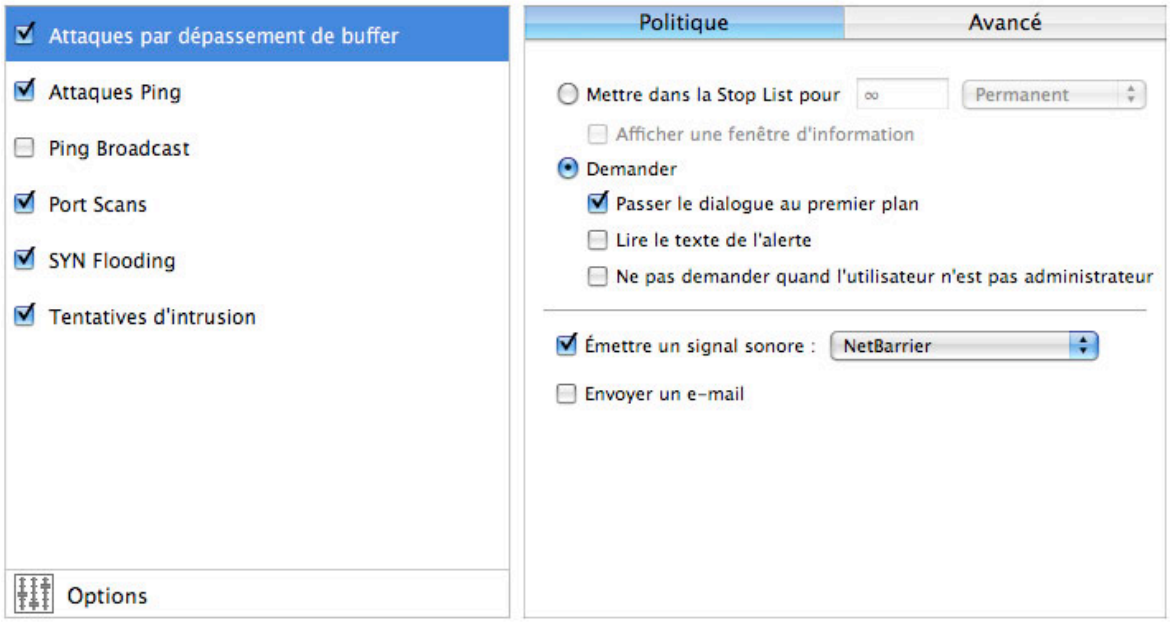
Le panneau Antivandale dispose d'outils de politiques pour éviter six types d'intrusions.



Attaques par dépassement de buffer	Attaques qui peuvent se produire lorsqu'un logiciel présente des défauts de gestion de mémoire.
Attaques Ping	Votre Mac reçoit un nombre ou une fréquence de demandes ping tellement élevés que le fait d'y répondre le mettrait à rude épreuve.
Ping Broadcast	Demandes ping de diffusion d'adresses, où un seul ping est multiplié à travers votre réseau local.
Port Scans	Tentatives, venant d'ordinateurs à distance, de recherche des vulnérabilités sur les ports de votre Mac. Si l'ordinateur fonctionne comme serveur, vous pouvez choisir de ne pas cocher cette case.
SYN Flooding	Multiples demandes TCP envoyées par un attaquant qui ne termine pas le stade final de l'échange, ce qui entraîne une forte consommation de ressources pour l'ordinateur cible.
Tentatives d'intrusion	Tentatives d'accès à votre Mac via un nombre préréglé de demandes de mot de passe incorrectes dans un délai de temps donné. Différents réglages concernent AppleShare IP (ASIP), FTP, HTTP, IMAP, POP et SMTP.

La protection contre chaque type d'intrusion est activée ou désactivée en cliquant sur la case qui l'accompagne. Quand on clique sur le nom du type d'intrusion, la politique de notification et d'action

est détaillée dans le panneau à droite. Voilà l'exemple de la politique pour les attaques par dépassement de buffer.



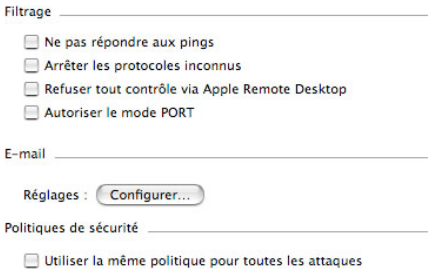
Ces options sont décrites au chapitre 9, **Comprendre les alertes**.

Un type d'intrusion étant sélectionné, des options spécifiques apparaissent quand on clique sur l'onglet Avancé du panneau à droite. Il s'agit des options suivantes :

Attaques par dépassement de buffer	Pas d'options avancées.
Attaques Ping	Sensibilité aux attaques Ping, mesurée en millisecondes (ms) permises entre les tentatives de ping. Si votre ordinateur est en réseau, il est normal que l'administrateur de système lui envoie des pings de temps en temps. Mais si votre ordinateur est isolé, les pings sont plus rares. Seule exception, en cas de connexion par câble ou DSL, le fournisseur d'accès Internet pourrait en envoyer pour vérifier si l'ordinateur est en ligne.
Ping Broadcast	Pas de réglages avancés.
Port Scans	Sensibilité ajustable sur une réglette, allant de faible à élevée, par incréments selon un calcul interne.
SYN Flooding	Sensibilité, mesurée en nombre de tentatives de connexions permises par seconde.
Tentatives d'intrusion	Réglage séparé du nombre de tentatives de mot de passe incorrect permises pour AppleShare IP (ASIP), FTP, HTTP, IMAP, POP et SMTP.

Options

Des options additionnelles de filtrage sont proposées dans le panneau Options de l'onglet Politique. Cliquez sur Options pour ajuster ces réglages.



Ne pas répondre aux pings	L'ordinateur est invisible aux autres ordinateurs sur Internet ou un réseau local. Cependant, il n'est pas anonyme ; toutes les demandes envoyées à d'autres hôtes portent son adresse IP.
Arrêter les protocoles inconnus	NetBarrier X5 bloque automatiquement tous les protocoles inconnus.
Refuser tout contrôle via Apple Remote Desktop	NetBarrier X5 bloque tous les accès à votre Mac venant du programme Apple Remote Desktop.
Autoriser le mode PORT	Vous pouvez effectuer des transferts FTP lors du fonctionnement en "Mode client" du Firewall.

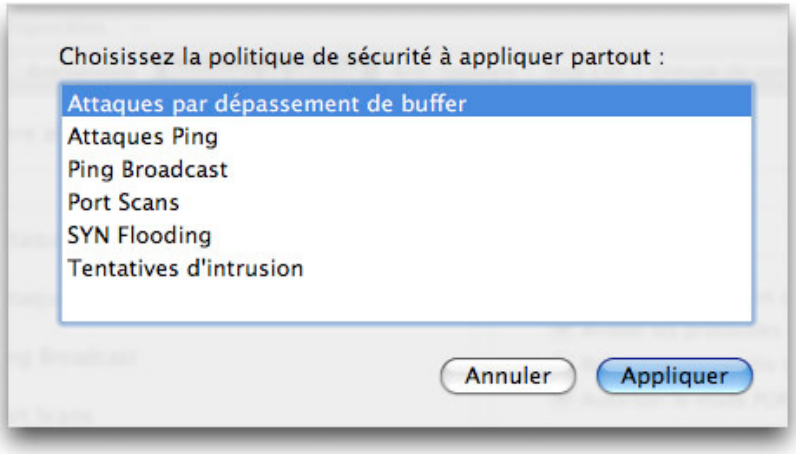
La seconde partie du panneau permet d'être notifié par message électronique, en cas de détection d'une attaque. Reportez-vous au chapitre 9, **Comprendre les alertes**, pour plus d'informations.

Unification des options de politique

Les réglages de chaque type d'intrusion déterminent le mode d'alerte et d'action, en cas de détection. Ces réglages sont détaillés au chapitre 9, **Comprendre les alertes**.

La case **Utiliser la même politique pour toutes les attaques** permet d'unifier toutes les notifications et actions. Quand cette case n'est pas cochée, vous pourriez, par exemple, choisir de recevoir un e-mail en cas de détection d'attaque de dépassement de buffer, mais de voir seulement une alerte en cas de tentative d'intrusion. En cochant cette case, NetBarrier X5 sait que vous voulez le même type de réponse, quel que soit le type d'intrusion.

Quand vous activez cette option, un dialogue demande quels réglages deviennent le modèle que les autres types d'intrusion vont suivre.



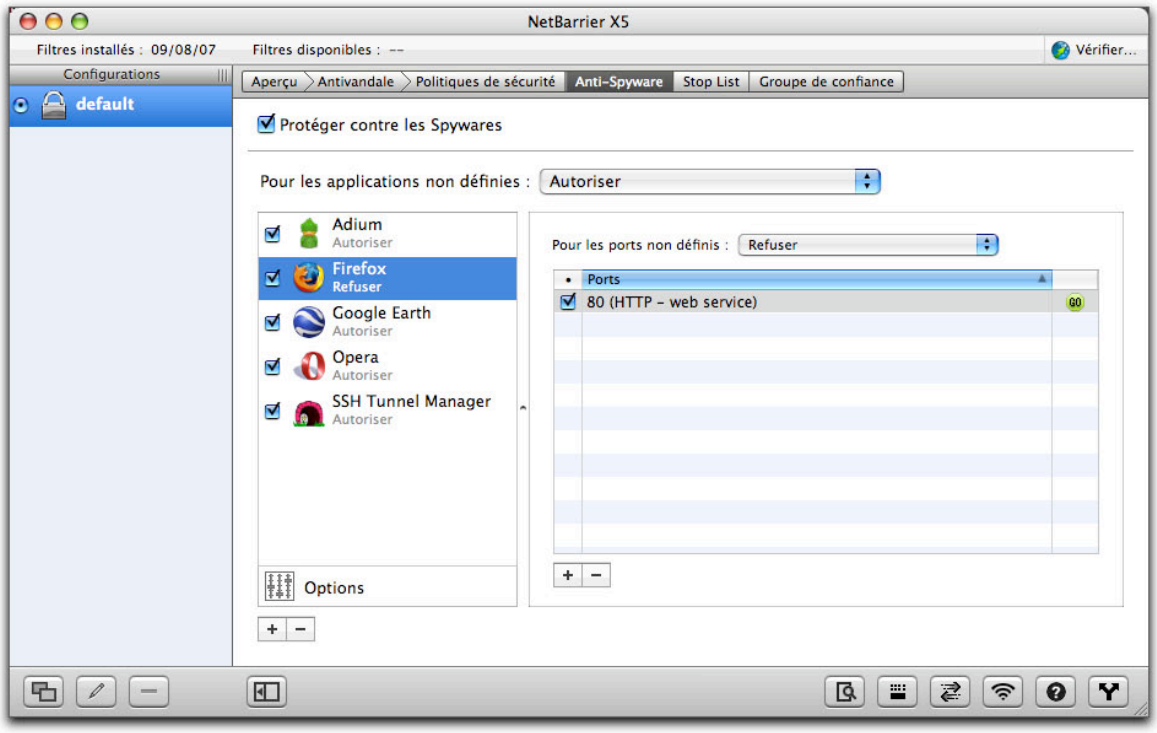
Anti-Spyware

NetBarrier X5 permet le contrôle, depuis votre Mac, de l'accès Internet et réseau, individualisé par application. Alors que les réglages de votre firewall peuvent autoriser l'accès général au réseau, le panneau Anti-Spyware permet de choisir le mode de réaction de NetBarrier X5 quand des applications spécifiques essaient d'avoir accès au réseau. Cette fonction présente deux intérêts :

- Pour éviter l'accès au réseau via certaines applications, vous pouvez bloquer celles-ci dans l'onglet Anti-Spyware.
- Si une application tente de se connecter au réseau à votre insu, NetBarrier X5 va l'arrêter, vous alerter et attendre que vous ayez décidé d'accepter ou de bloquer l'accès.

Votre Mac dispose de plusieurs applications ayant accès à Internet ou à d'autres réseaux : navigateurs web, programmes de messagerie, programmes FTP (transfert de fichier) et applications de messagerie instantanée. Cependant, il peut exister des programmes se connectant au réseau sans vous prévenir, afin de vérifier les numéros de série des logiciels installés sur l'ordinateur, rassembler et transmettre des informations personnelles à votre insu, ou ouvrir une porte dérobée sur votre Mac et laisser la voie libre aux pirates et autres vandales. NetBarrier X5 vous notifie à chaque tentative et vous laisse décider de la suite à donner.

Pour activer le blocage d'application, cochez la case **Protéger contre les Spywares** en haut du panneau Anti-Spyware.

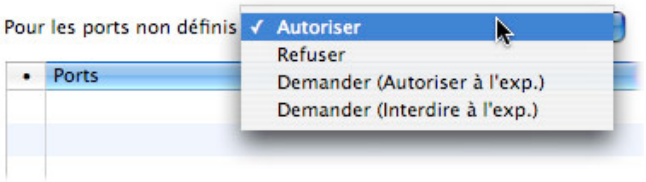


L'Anti-Spyware demande d'abord de préparer la liste des applications auxquelles vous voulez appliquer des réglages. Il s'agit des applications "définies", toutes celles qui ne sont pas dans la liste étant considérées "non définies". Dans l'exemple ci-dessus, Google Earth est défini, alors qu'Internet Explorer (qui n'est pas dans la liste) est non défini.

Dès que vous avez établi cette liste, vous pouvez contrôler finement les communications venant d'applications définies et fixer une politique générale pour les communications venant d'applications non définies. Précisons deux configurations habituelles :

- Vous gérez une salle d'informatique et vous voulez que les étudiants puissent envoyer des e-mails à l'aide du programme Mail d'Apple, mais ne puissent pas naviguer sur le web ni jouer à des jeux en réseau. Vous allez définir Mail comme autorisé, et refuser toutes les connexions sortantes venant des autres programmes.
- Vous suspectez qu'une application que vous avez téléchargée sur votre Mac envoie des communications non autorisées, peut-être à partir d'un spyware caché, intégré au programme. Vous allez définir ce programme et refuser toutes les communications qu'il émet, et vous autorisez toutes les communications venant des applications non définies.

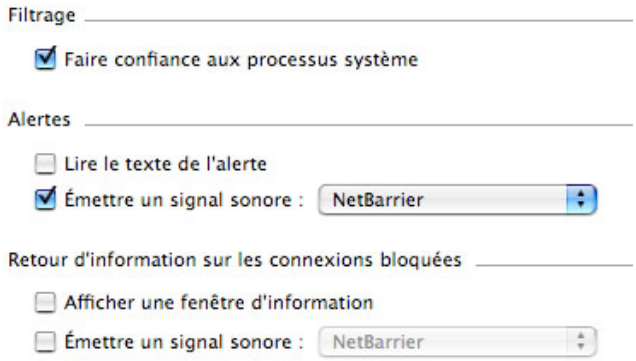
Quatre options de comportement sont disponibles pour les applications non définies :



Autoriser	NetBarrier X5 autorise l'accès à Internet ou à tout autre réseau à toutes les applications. Cependant, toutes les règles de firewall préalablement définies et concernant l'accès entrant ou sortant de ports spécifiques restent applicables. Par exemple, si un programme FTP essaie de se connecter à une page web, NetBarrier X5 ne bloque pas l'application, mais si vous avez mis en place une règle de firewall bloquant le port 20 (port FTP standard), les données ne passent pas. Si le programme FTP tente de se connecter à un port différent, il n'est pas bloqué.
Refuser	NetBarrier X5 bloque tout accès à Internet ou à tout autre réseau. Cette option prévaut sur toutes les règles de firewall que vous avez définies.
Demander (Autoriser à l'exp.)	NetBarrier X5 vous consulte à chaque tentative de connexion à Internet ou à tout autre réseau. Si vous ne répondez pas dans un délai de 90 secondes, l'application est autorisée, pour cette fois seulement, à avoir accès à Internet.
Demander (Interdire à l'exp.)	NetBarrier X5 vous consulte à chaque tentative de connexion à Internet ou à tout autre réseau. Si vous ne répondez pas dans un délai de 90 secondes, l'application a un refus d'accès, pour cette fois seulement.

Options

Le bouton Options, en bas à gauche du panneau Anti-Spyware, permet la configuration de quelques réglages Anti-Spyware généraux.



La seule option spécifique à l'Anti-Spyware est Faire confiance aux processus système, ce qui permet les communications venant des nombreux éléments du Mac OS X lui-même qui demandent l'accès Internet ou réseau. Ces demandes peuvent concerner les services d'impression, la résolution de nom de domaine, les vérifications pour les mises à jour de logiciels ou la synchronisation d'horloge. Ces demandes viennent d'éléments du système Mac OS X, et non pas d'applications séparées. Pour permettre ces processus, et éviter les questions lors de leur tentative de connexion à Internet ou au réseau, cochez la case **Faire confiance aux processus système**.

Pour des détails sur les autres options de l'Anti-Spyware, reportez-vous au chapitre 9, **Comprendre les alertes**.

Applications : Ajout, suppression et modification de réglages

Après avoir choisi d'autoriser ou d'interdire l'accès réseau aux applications non définies, vous définissez une application en cliquant sur le bouton +, puis en naviguant via le dialogue Mac OS X vers l'application elle-même pour l'ajouter. Répétez le processus pour toutes les applications à ajouter. (Pour supprimer une application de la liste, cliquez dessus, puis sur le bouton – au bas de la liste.)

Vous pouvez ensuite modifier les réglages de chaque application, pour autoriser ou bloquer les communications de l'application dans son ensemble, ou sur des ports spécifiques. De façon similaire au processus ci-dessus, où vous spécifiez ce qui se passera quand des applications non définies tentent des communications sortantes, vous définissez ici ce qui se passera quand une application spécifique tente d'établir une communication venant d'un port non défini. Puis vous définissez, pour cette application spécifique, une liste des ports qui font exception à la règle générale.

Dans l'exemple ci-dessus :

- Cinq applications (listées à gauche) sont soumises à des règles spécifiques ; les connexions sortantes, venant de toutes les autres applications, sont autorisées.
- Firefox est autorisé à envoyer deux catégories de communications, via les ports 80 et 8080.
- Les communications par Firefox via le port 443 sont interdites.
- Les communications par Firefox via tout autre port génèrent une alerte sur l'écran de votre Mac ; si vous ne répondez pas dans un délai de 90 secondes, la connexion est refusée.

La liste des ports comporte trois colonnes :

- La première colonne, avec des cases à cocher, indique le comportement du port qui est activé pour l'application. Si la case est cochée, le comportement spécifié est actif. Décochez la case si vous souhaitez désactiver ce comportement. Vous pourrez le réactiver ultérieurement.
- La deuxième colonne, Ports, donne des informations relatives aux ports via lesquels l'application a accès au réseau. Elle indique le numéro de port et, dans certains cas, le protocole mis en œuvre et une brève description. (Cette description apparaît automatiquement quand vous entrez un numéro de port que NetBarrier X5 reconnaît.) Vous pouvez ajouter un numéro de port, ou un intervalle de numéros de port, par exemple, 110-123.
- La troisième colonne comporte une icône : soit l'icône GO, verte, indiquant que l'accès réseau est autorisé ; soit l'icône STOP, rouge, indiquant l'interdiction d'accès.

- Pour modifier le réglage, il suffit de cliquer sur l'icône verte, GO, et elle devient STOP, en rouge. De même, vous pouvez basculer de STOP à GO.

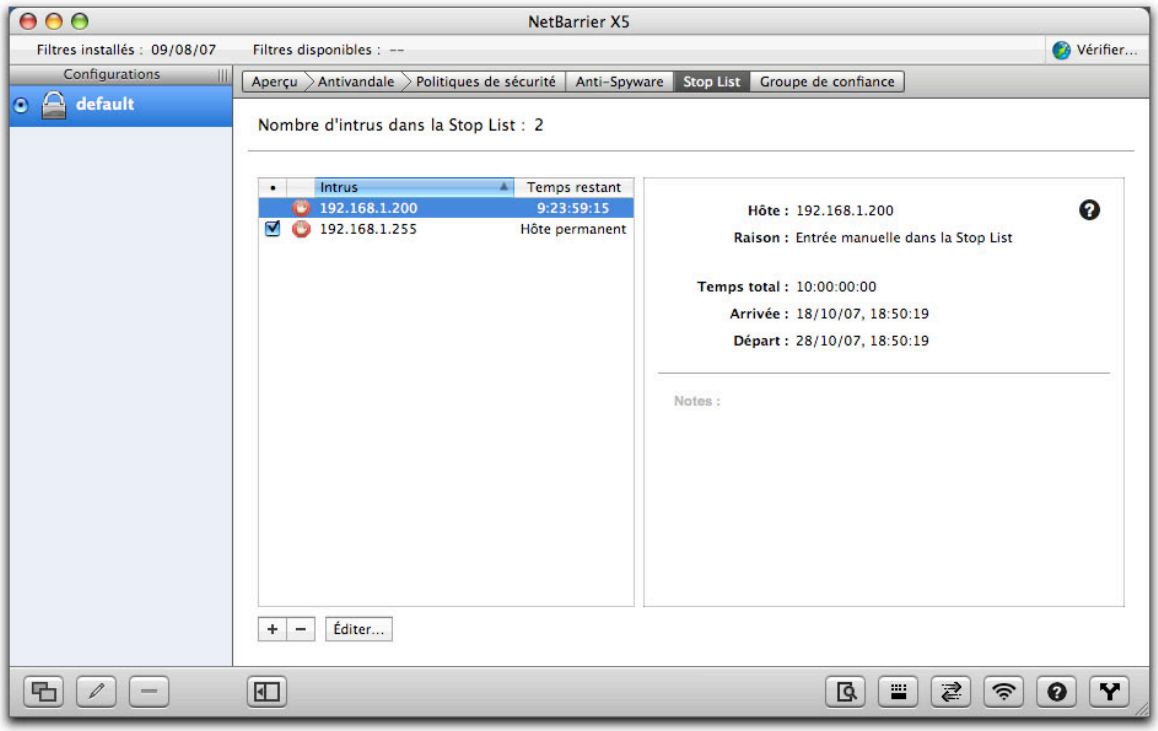
Pour voir une application de la liste dans le Finder, maintenez la touche Ctrl enfoncée et cliquez sur le nom d'une application. Un menu contextuel apparaît. Sélectionnez Afficher dans le Finder, et une fenêtre de Finder s'ouvre, précisant l'emplacement de l'application.

Stop List et Groupe de confiance

La Stop List assure qu'une fois la tentative d'attaque ou d'intrusion déjouée, aucune communication ne se produira entre la machine attaquante et votre Mac pendant la durée que vous définissez.

Le Groupe de confiance est l'opposé de la Stop List : il liste les ordinateurs "amis" qui *sont* autorisés à se connecter à votre Mac. Alors que la Stop List vous protège de vos ennemis, le Groupe de confiance ouvre la porte à vos amis. L'Antivandale de NetBarrier X5 ne bloquera pas l'accès aux ordinateurs listés dans le Groupe de confiance, ni ne déclenchera d'alertes du fait de leurs actions. Cependant, les ordinateurs du Groupe de confiance restent sensibles à toutes les règles actives du Firewall.

L'interface du panneau Groupe de confiance est très similaire à celle du panneau Stop List, nous allons les examiner en même temps, en insistant sur les différences éventuelles. Voici le panneau de la Stop List, avec quelques échantillons de données :

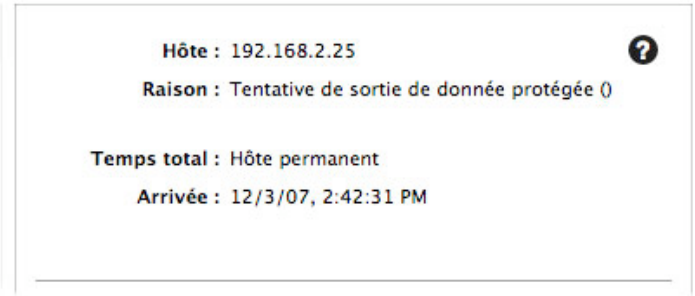


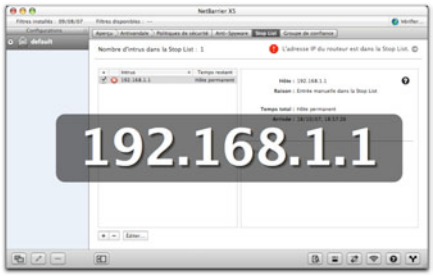
Le panneau à gauche comprend les éventuelles adresses IP présentes dans la Stop List ou le Groupe de confiance.

Case à cocher	Vous pouvez désactiver temporairement un élément de la Stop List/du Groupe de confiance en décochant cette case, qui est cochée par défaut lors de l'ajout aux listes. Quand l'élément est désactivé, vous le réactivez en cliquant dessus. (Cette case apparaît seulement si l'adresse IP est réglée en blocage permanent.)
Intrus/Hôte	La seconde colonne contient l'adresse IP intruse (dans la Stop List) ou permise (dans le Groupe de confiance).
Temps restant	Si vous avez réglé cette adresse IP pour qu'elle soit interdite/permise pour une durée spécifique, cette colonne indique le temps restant, à la seconde près. Sinon, la colonne indique "Hôte permanent", et l'adresse IP va rester jusqu'à la suppression manuelle.

Informations contenues dans la Stop List/le Groupe de confiance

Si vous cliquez sur un élément de la Stop List/du Groupe de confiance, des informations supplémentaires apparaissent sur la droite du panneau.



Hôte	Adresse IP de l'hôte. En cliquant sur le bouton de recherche DNS (le **?**), vous basculez de l'adresse IP numérique au nom de domaine de l'attaquant, le cas échéant. (voir **Note à propos des recherches DNS**.) Pour l'affichage de l'adresse en gros caractères, déplacez le curseur sur le mot Hôte jusqu'à ce qu'il soit mis en surbrillance, puis cliquez et sélectionnez Grande police dans le menu contextuel qui apparaît. Le résultat a l'aspect suivant : 
Raison	Pourquoi l'adresse IP a été ajoutée à la Stop List. Ce texte n'apparaît pas dans le panneau du Groupe de confiance, vu que tous les éléments y sont ajoutés manuellement.
Temps total	C'est la durée pendant laquelle l'ordinateur va rester dans la Stop List/le Groupe de confiance. En cliquant sur les mots Temps total, le Temps restant va s'afficher ; en cliquant à nouveau, on obtient le Temps écoulé, indiquant la durée de présence de l'attaquant dans la Stop List. En cliquant sur Temps écoulé, le Temps total va à nouveau s'afficher.
Arrivée	Moment où l'adresse IP a été ajoutée à la Stop List/au Groupe de confiance.
Départ	Si vous avez précisé une durée de séjour d'une adresse IP dans la Stop List/le Groupe de confiance, le moment du départ va s'afficher.

Notes	Tous les commentaires que vous avez entrés pour cette adresse IP. NetBarrier X5 ajoute automatiquement des commentaires à ce champ quand il place un élément dans la Stop List, comme dans l'exemple ci-dessus.

Note à propos des recherches DNS

Vous constatez, en divers endroits dans NetBarrier X5, un bouton avec un point d'interrogation sur fond sombre. En cliquant dessus, les informations voisines basculent de l'adresse IP numérique au nom de domaine associé, et vice versa.

Attention, les adresses IP n'ont pas de relation univoque aux noms de domaine. Par exemple, un domaine important pourrait avoir www.example.com hébergé sur une adresse IP, forums.example.com hébergé sur une autre, et blog.example.com hébergé sur une troisième adresse.

Cependant, les petits domaines partagent souvent une même adresse IP avec d'autres, tous étant hébergés comme "domaines virtuels" sur un seul ordinateur. Dans ces cas, la recherche de domaine donne une adresse IP qui conduit en fait au nom d'une machine plus importante et inattendue, par exemple, apache2-vat.marketstreet.example.com.

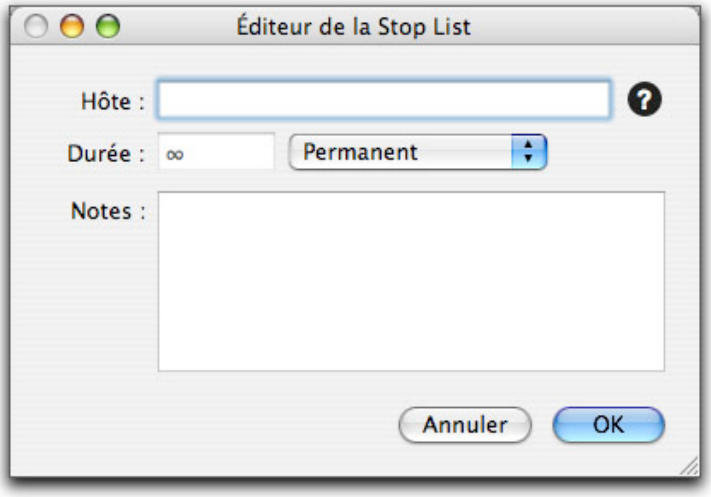
En résultat, le fait d'entrer une adresse IP pourrait bloquer (ou autoriser) du trafic venant de domaines inattendus, tandis que le fait d'entrer un domaine pourrait ne pas bloquer (ou ne pas autoriser) tout le trafic désiré. Cela relève de la structure des domaines sur Internet, non pas d'une erreur de NetBarrier X5. Si vous constatez des problèmes avec du trafic bloqué ou autorisé de manière inattendue, essayez d'utiliser un nom de domaine au lieu d'une adresse IP, ou vice versa.

Ajout d'adresses

Deux modes existent pour l'ajout manuel d'adresses à la Stop List/au Groupe de confiance. (NetBarrier X5 peut automatiquement ajouter des adresses à la Stop List en réponse à des alertes. Pour plus de détails, reportez-vous au chapitre 9, **Comprendre les alertes**.)

Le premier mode est la sélection d'une adresse IP dans la fenêtre de l'Historique, et le choix Ajouter à la Stop List dans le menu contextuel. Pour en savoir plus, reportez-vous au chapitre 8, **Les Quatre lignes de défense : Supervision**.

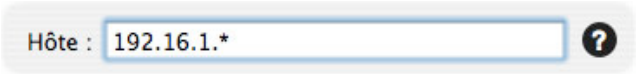
Vous pouvez aussi ajouter manuellement des adresses à la Stop List/au Groupe de confiance. Pour cela, cliquez sur le bouton **+** au bas de la liste. Une fenêtre apparaît.



Entrez l'adresse de l'hôte dans le champ Hôte, puis choisissez la durée de maintien de l'adresse dans la Stop List (ou le Groupe de confiance) en entrant un nombre dans le champ Durée. Choisissez l'unité de temps dans le menu déroulant. Si vous ne connaissez pas l'adresse IP numérique de l'hôte que vous souhaitez ajouter, entrez son nom et cliquez sur le bouton **?**. NetBarrier X5 interroge alors le serveur DNS de votre fournisseur d'accès Internet, et entre le numéro correct dans le champ. (Voir la **Note à propos des recherches DNS**.) Un champ de notes est prévu pour vos commentaires, tels que la raison de l'ajout. Si vous décidez de ne pas ajouter cette adresse à la Stop List/au Groupe de confiance, cliquez sur Annuler.

Utilisation de jokers

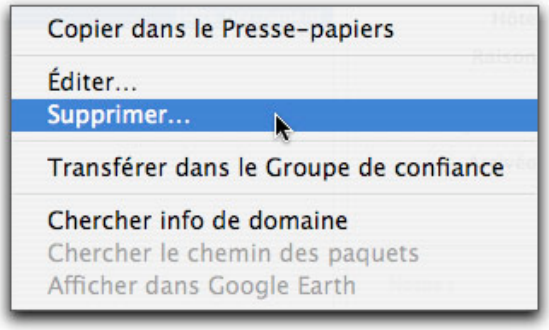
L'utilisation de jokers permet d'indiquer des intervalles d'adresses IP dans la Stop List ou le Groupe de confiance. Pour cela, entrez la première partie de l'adresse IP à bloquer, suivie d'astérisques. Par exemple, 192.168.1.* va bloquer toutes les adresses IP de 192.168.1.0 à 192.168.1.255 inclus ; 192.168.*.* va bloquer les adresses IP de 192.168.[0-255].[0-255] ; et ainsi de suite.



Suppression d'adresses

Pour supprimer une adresse de la Stop List/du Groupe de confiance, cliquez sur l'adresse concernée, puis cliquez sur le bouton -. Un dialogue demande de confirmer la suppression.

Vous pouvez également supprimer une adresse en cliquant dessus tout en maintenant la touche Ctrl enfoncée, puis en sélectionnant Supprimer… dans le menu contextuel qui apparaît. Un dialogue demande de confirmer la suppression.



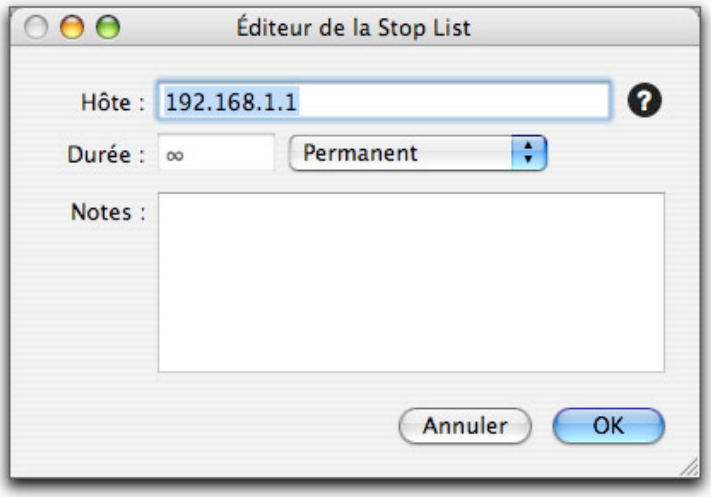
Transfert d'adresses entre la Stop List et le Groupe de confiance

Vous pouvez décider du transfert d'adresse de la Stop List vers le Groupe de confiance, ou vice versa. Pour cela, maintenez la touche Ctrl enfoncée, puis sélectionnez Transférer dans le Groupe de confiance, ou Transférer dans la Stop List, dans le menu contextuel qui apparaît.

Modification d'une adresse

Il existe trois façons de modifier une adresse dans la Stop List/le Groupe de confiance :

- Cliquez sur l'adresse concernée, puis cliquez sur le bouton Éditer... en bas à gauche du panneau.
- Double-cliquez sur l'adresse ; ou
- Cliquez sur l'adresse tout en maintenant la touche Ctrl enfoncée, puis sélectionnez Éditer… dans le menu contextuel.



L'Éditeur de la Stop List/du Groupe de confiance apparaît. Vous pouvez modifier l'adresse, ajouter ou modifier les notes, ou modifier la durée de maintien dans la Stop List/le Groupe de confiance.

Menu Contextuel

Comme vous venez de le voir, vous pouvez cliquer sur un élément de la Stop List/du Groupe de confiance tout en maintenant la touche Ctrl enfoncée, pour faire apparaître un menu contextuel. Nous allons préciser les quatre autres fonctions de ce menu : Copier dans le Presse-papiers, Chercher info de domaine, Chercher le chemin des paquets, Afficher dans Google Earth.

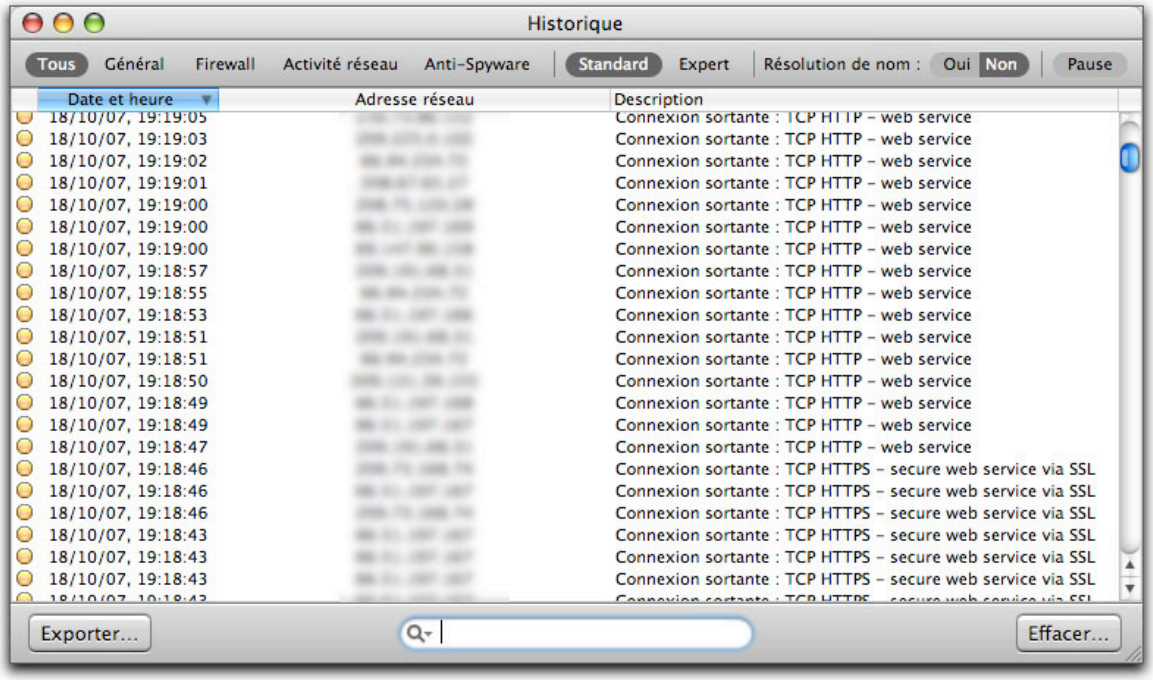
Copier dans le Presse-papiers	Pour placer l'adresse IP sur le Presse-papiers de Mac OS X, où elle peut être collée dans d'autres programmes (comme un traitement de texte).
Chercher info de domaine	Pour ouvrir la fenêtre Whois de NetBarrier X5 et faire des recherches sur l'adresse IP sélectionnée. Consulter le chapitre 8, **Les Quatre lignes de défense : Supervision** pour plus d'infos.
Chercher le chemin des paquets	Pour ouvrir la fenêtre Traceroute de NetBarrier X5 et faire des recherches sur l'adresse IP sélectionnée. Consulter le chapitre 8, **Les Quatre lignes de défense : Supervision** pour plus d'infos.
Afficher dans Google Earth	Pour lancer le programme Google Earth et tenter de trouver l'emplacement géographique de l'adresse IP sélectionnée. Consulter le chapitre 8, **Les Quatre lignes de défense : Supervision** pour plus d'infos.

8 - Les Quatre lignes de défense : Supervision

Historique

L'historique présente l'enregistrement de toute l'activité de NetBarrier X5. Il liste chaque occurrence d'incident, l'adresse de l'intrus et le type d'incident enregistré. Pour accéder à l'historique, cliquez sur la petite icône de "loupe" au bas du panneau, choisissez Fenêtre > Historique, ou tapez Option-Commande-L.

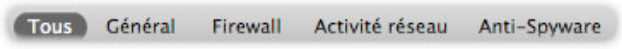
Vous arrivez à l'interface principale de l'historique. Vos entrées seront forcément différentes de l'exemple ci-dessous, elles vont refléter l'activité sur votre Mac depuis que vous avez installé NetBarrier X5 (ou depuis le dernier effacement de l'historique).



Options d'affichage de l'historique

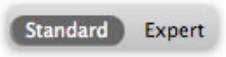
Le haut du panneau d'historique contient trois groupes d'options qui affectent son apparence. Le premier groupe présente des sous-ensembles d'activité de l'historique, pour vous aider à étudier plus facilement des problèmes potentiels ; le second groupe bascule entre la vue par défaut Standard et une vue étendue Expert ; le troisième groupe laisse le choix entre l'affichage des adresses IP brutes ou des noms de domaine selon la recherche DNS. Nous allons traiter chaque groupe d'options séparément.

Les activités se répartissent en trois groupes : Général, Firewall et Activité réseau. Vous pouvez choisir de voir les activités relatives à tous les groupes en même temps, ou seulement les activités relatives à un groupe spécifique. Cliquez sur l'un des boutons dans la barre pour modifier l'affichage de l'historique.

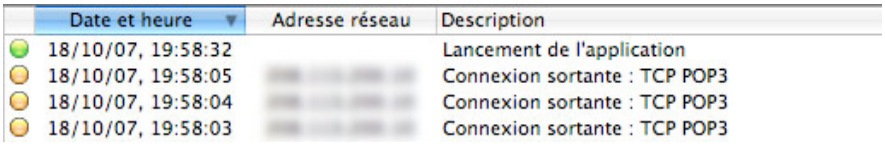


Tous	Toute l'activité tracée par NetBarrier X5. C'est le réglage par défaut.
Général	Activité relative au fonctionnement de NetBarrier X5 lui-même, telle que les cas où vous avez lancé et terminé le programme, ajouté des applications à l'Anti-Spyware, entré des éléments dans la Stop List et le Groupe de confiance, et ainsi de suite.
Firewall	Incidents quand l'activité réseau a fait intervenir une règle du Firewall, pour laquelle l'historique était activé. Les enregistrements des attaques de chevaux de Troie apparaissent aussi dans l'historique, si vous avez activé la protection contre les Troyens.
Activité réseau	Toutes les connexions aux réseaux ou à Internet, et quand les adresses IP de la Stop List ont tenté de se connecter à votre ordinateur.
Anti-Spyware	Sous-groupe du groupe Général, indiquant seulement l'ajout ou la suppression d'applications dans la liste Anti-Spyware, ou l'intervention de règles Anti-Spyware.

Affichage de l'historique en mode standard ou expert

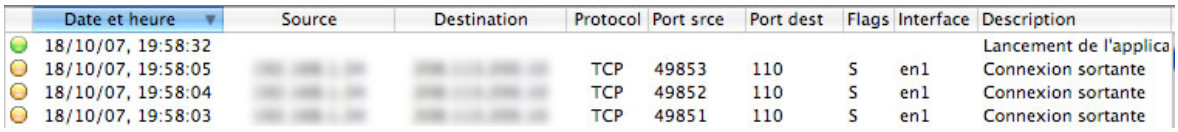


Standard : C'est l'affichage par défaut du panneau de l'historique. Il indique quatre éléments d'informations pour chaque entrée de l'historique.



- Le type d'activité, selon la couleur de la pastille :
    - Verte : Général
    - Jaune : Firewall
    - Rouge : Réseau
- La date et l'heure de l'activité, selon le réglage d'horloge de votre Mac.
- L'adresse réseau, donnée en adresse IP, par défaut. Si vous avez coché la résolution de nom (voir ci-dessous), les noms de domaine apparaissent pour les adresses que NetBarrier X5 a pu résoudre.
- La description rapide de l'activité.

Expert : C'est un affichage étendu, indiquant les champs suivants, le cas échéant.



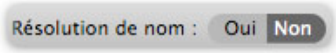
- Le type d'activité, selon la description ci-dessus.
- La date et l'heure de l'activité.
- L'adresse de la source, avec l'adresse IP (ou le domaine) de l'origine de l'incident. Pour la plupart des activités, la source sera l'adresse IP de votre Mac ; ce sera l'adresse de

l'ordinateur offensif, en cas d'attaque. Si vous avez coché Résolution de nom, les noms de domaine apparaissent pour les adresses que NetBarrier X5 a pu résoudre.

- L'adresse de la destination, rédigée en adresse IP, par défaut.
- Le protocole, indiquant le mode de la tentative de connexion, c'est-à-dire, TCP, UDP, ICMP ou IGMP.
- Port source ; le port duquel les données sont envoyées.
- Port destination ; le port prévu pour les données.
- Les drapeaux (flags) TCP apparaissent : A (acquittement), S (synchronisation), F (fin des données), ou R (reset).
- Interface ; l'interface réseau servant à l'envoi des données, telle que Ethernet ou AirPort, indiquée en nom BSD.
- Description, une description rapide de l'activité.

Les activités générales, telles que le lancement ou l'arrêt du programme NetBarrier X5, ne concernent pas d'autres ordinateurs que votre Mac, et n'indiquent donc pas tous les champs liés à l'activité réseau.

Résolution du nom de domaine



NetBarrier X5 vous aide à retrouver la trace des intrus en résolvant les noms de domaine de vos connexions. Les adresses Internet existent sous deux formes : en nombres IP, tels que 192.168.1.1, et alphabétique, tel que exemple.com. La correspondance entre les deux est enregistrée sur les serveurs de noms de domaine répartis sur tout le réseau Internet.

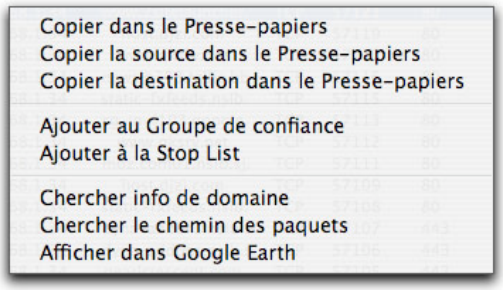
Quand la case **Résolution de Nom** est cochée dans le panneau Historique, NetBarrier X5 essaie de trouver les noms correspondant aux adresses Internet présentées dans l'historique. Si NetBarrier X5 peut trouver ces informations, le domaine est alors affiché sous forme alphabétique.

Date et heure	Adresse réseau	Description
18/10/07, 20:27:39	kc-in-f91.google.com	Connexion sortante : TCP HTTP – web service
18/10/07, 20:27:07	cg-in-f103.google.com	Connexion sortante : TCP HTTP – web service
18/10/07, 20:27:06	cg-in-f97.google.com	Connexion sortante : TCP HTTPS – secure web service via SSL
18/10/07, 20:27:04	www.intego.com	Connexion sortante : TCP HTTP – web service

NetBarrier X5 ne peut pas résoudre toutes les adresses Internet, puisque certaines n'ont pas d'équivalent alphabétique. Pour plus d'information, voir la **Note à propos des recherches DNS**.

Menu contextuel de la fenêtre de l'historique

Si vous maintenez la touche Ctrl enfoncée et cliquez sur une ligne de l'historique, un menu contextuel apparaît.

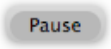


Les options sont les suivantes :

Copier dans le Presse-papiers	Pour copier les colonnes visibles de cette entrée de l'historique sur le presse-papiers du Mac OS X, au format texte avec tabulation. Vous pouvez ensuite les coller dans une autre application ou un document.
Copier la source dans le Presse-papiers	Pour copier seulement le champ Source de cette entrée de l'historique sur le presse-papiers du Mac OS X : disponible lors de l'affichage de l'historique en mode Expert.
Copier la destination dans le Presse-papiers	Pour copier seulement le champ Destination de cette entrée de l'historique sur le presse-papiers du Mac OS X : disponible lors de l'affichage de l'historique en mode Expert.
Ajouter au Groupe de confiance	Pour l'ajout permanent de cette adresse IP est ajoutée au Groupe de confiance, permettant les connexions futures, indépendamment des réglages de l'Antivandale. Cependant, le Firewall de NetBarrier X5 affecte toujours les communications venant de cette adresse IP.
Ajouter à la Stop List	Pour l'ajout permanent de cette adresse IP est ajoutée à la Stop List, bloquant les connexions futures, indépendamment des réglages de l'Antivandale. Cependant, le Firewall de NetBarrier X5 affecte toujours les communications venant de cette adresse IP.
Chercher info de domaine	Pour lancer la fenêtre Whois de NetBarrier X5 et faire des recherches sur l'adresse IP sélectionnée. Consulter **Whois** pour plus d'infos.
Chercher le chemin des paquets	Pour lancer la fenêtre Traceroute de NetBarrier X5 et faire des recherches sur l'adresse IP sélectionnée. Consulter **Traceroute** pour plus d'infos.

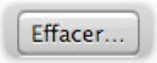
Afficher dans Google Earth	Pour lancer le programme Google Earth, s'il est installé, et tenter de trouver l'emplacement géographique de l'adresse IP sélectionnée.

Pause de l’historique



Si de nombreuses connexions entrent et sortent de l’ordinateur, il devient difficile de suivre l’historique au fur et à mesure qu’il s’affiche. Pour faciliter la consultation, cliquez sur le bouton Pause dans le coin supérieur droit du panneau. L’affichage s’arrête et vous pouvez lire les données ; cependant, l'enregistrement des données continue et l'affichage reprend dès la fin de la pause. Pour revenir à l’affichage en temps réel, cliquez à nouveau sur le bouton Pause.

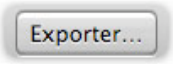
Effacement de l'historique



Pour effacer l’historique et vider toutes les informations stockées, cliquez sur Effacer... dans le coin inférieur droit du panneau. Un dialogue demande de confirmer la suppression.

L'historique est automatiquement effacé si vous avez coché la case **Effacer l'historique après l'export** dans les Préférences, et si NetBarrier X5 est réglé pour l'export périodique d'un historique. Consulter le chapitre 10, **Préférences et configurations**.

Export de l'historique

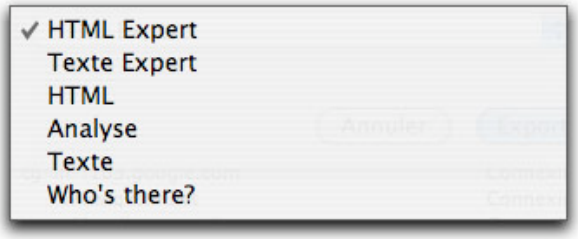


Les données de l'historique sont exportables selon plusieurs formats : Lors d'un export manuel, seules les données affichées sont exportées - si vous n'avez coché que Firewall, par exemple, dans le panneau Historique, seules les données de Firewall sont exportées. (Vous pouvez choisir l'export automatique des données de l'historique : Consulter le chapitre 10, **Préférences et configurations**.)

Pour exporter les données de l'historique, cliquez sur le bouton **Exporter…**. Un dialogue demande d'enregistrer le fichier ; vous pouvez alors en changer le nom. Choisissez le dossier où vous souhaitez l'enregistrer - par défaut, tous les fichiers d'export sont enregistrés dans votre dossier <</Library/Logs/NetBarrier.

ATTENTION : Si la fonctionnalité de résolution de domaine est activée, les exports d'historique peuvent durer plusieurs minutes.

Les historiques sont exportables selon six formats ; pour la sélection, cliquez dans le menu déroulant Format.



Les formats disponibles sont les suivants :

HTML Expert	Format HTML, indiquant toutes les colonnes visibles en mode Expert. Dans ce format vous pouvez partiellement retracer l'historique de navigation, vu que NetBarrier X5 fournit des liens actifs vers toutes les tentatives pour atteindre des pages web non sécurisées. (C'est-à-dire, les ports de destination, connectés par TCP, visant les ports 80 ou 8080.)
Texte Expert	Format texte simple, avec tabulation, indiquant toutes les colonnes visibles

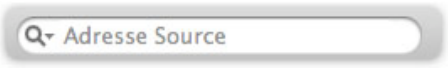
	en mode Expert. C'est le mode de choix pour l'import dans un programme de feuille de calcul ou de base de données.
HTML	Format HTML, indiquant toutes les colonnes visibles en mode Standard. Comme pour les exports en HTML Expert, ce format de fichier aide à retracer l'historique de navigation.
Analyse	Format texte similaire à Texte Expert, sans séparateurs de tabulation, mais avec des étiquettes devant certains champs.
Texte	Format texte simple, avec tabulation, indiquant toutes les colonnes visibles en mode Standard.
Who's there?	L'historique en fichier texte, avec les colonnes suivantes : Date, Heure, Résultat, Hôte, Port serveur et Méthode ; mode utile dans certains programmes d'analyse d'historique.

Filtrage des données dans la fenêtre de l'historique

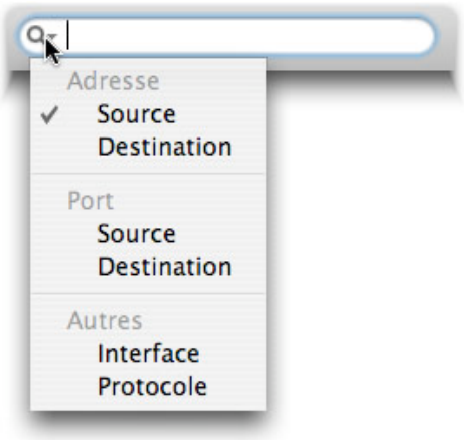
Au bas de la fenêtre de l'historique, un champ de recherche permet de filtrer les données selon plusieurs critères, en n'affichant que les lignes contenant les critères choisis dans les catégories suivantes :

- **Adresse Source**
- **Adresse Destination**
- **Port Source**
- **Port Destination**
- **Interface**
- **Protocole**

L'adresse Source est le critère par défaut, comme l'indique le champ de recherche.

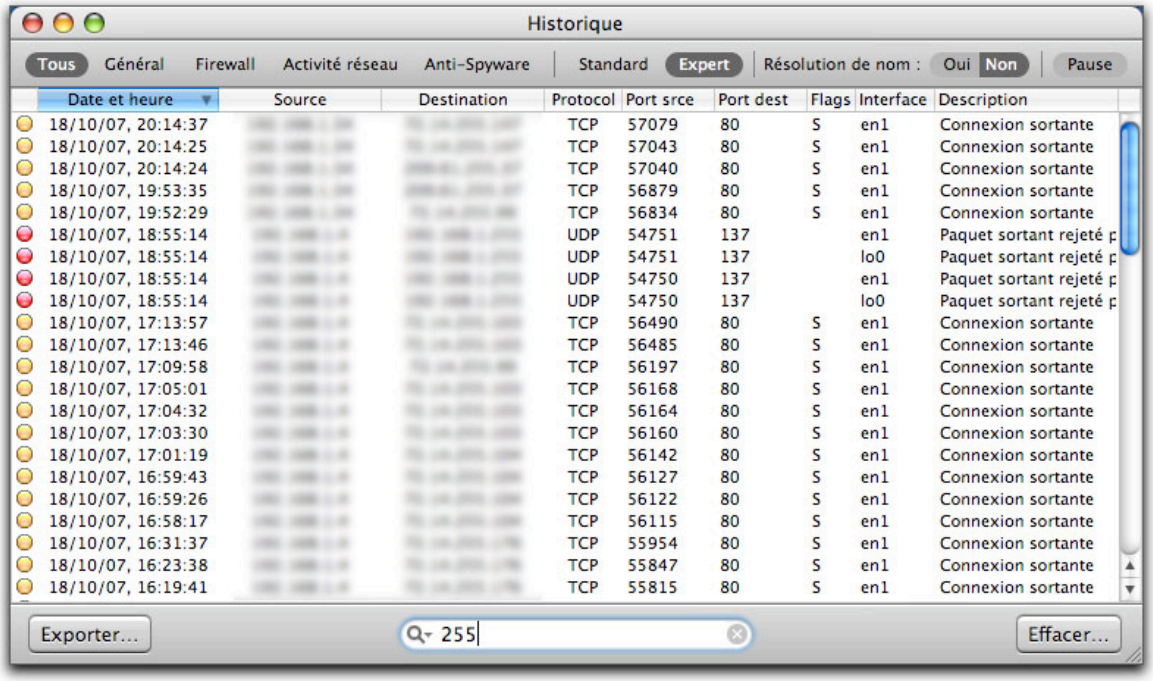


Pour rechercher les données de l'historique contenant l'un de ces critères, cliquez sur le triangle à côté de l'icône de recherche.



Sélectionnez le critère à rechercher, puis entrez une chaîne dans le champ de recherche. Vous n'avez pas besoin d'entrer toute la chaîne ; l'affichage est dynamique et réduit automatiquement les données de l'historique quand vous entrez les caractères dans le champ de recherche.

Dans l'exemple ci-dessous, nous avons recherché "255" dans l'adresse de destination. Peu importe l'emplacement du texte cherché, même s'il n'est pas au début. La recherche fonctionne, même si vous affichez l'historique en mode Standard, où le champ de recherche (dans ce cas, la Destination) peut se trouver masqué.



Pour effacer le contenu du champ et passer à une nouvelle recherche, cliquez sur le petit bouton d'effacement "x" à droite du champ.

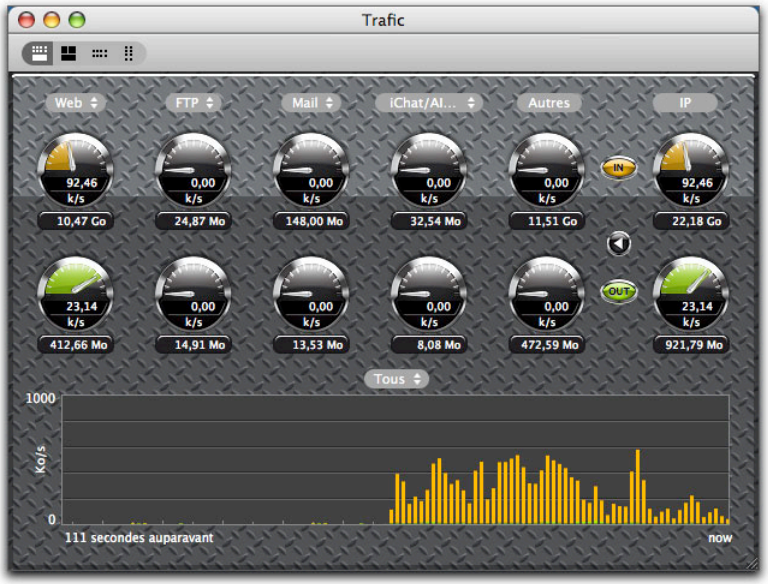
Trafic

Le panneau Trafic dispose d'un jeu de compteurs d'activité, qui indiquent le type et la quantité d'activité réseau transitant par votre Mac et venant d'Internet et des réseaux locaux. Pour accéder au panneau Trafic, cliquez sur la petite icône présentée ci-dessous, choisissez Fenêtre > Trafic, ou tapez Option-Commande-1.

Modes d'affichage du trafic

Le panneau Trafic dispose de quatre modes d'affichage, sélectionnés en cliquant sur les petits boutons en haut du panneau.

Le premier bouton est l'affichage par défaut, où le trafic est présenté en deux rangées de compteurs et un histogramme.

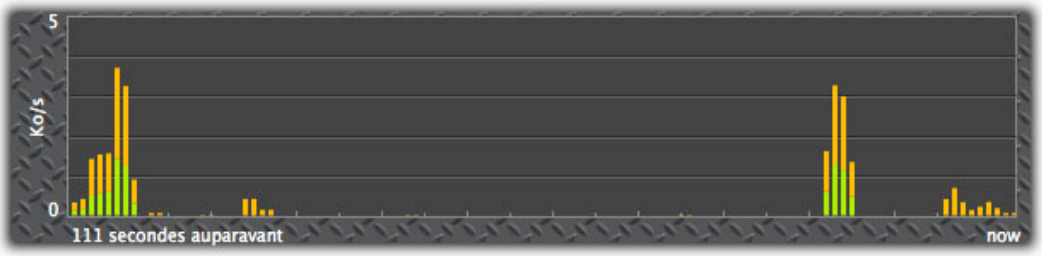


Les compteurs IN, en haut, avec les valeurs en orange par défaut, indiquent la quantité de données entrant dans votre Mac. Les compteurs OUT, en bas, avec les valeurs en vert par défaut, indiquent la quantité de données sortant de votre Mac. Dans chaque compteur, le nombre à l'intérieur indique le débit par seconde, et le nombre au-dessous indique la quantité totale, généralement en mégaoctets (Mo) ou gigaoctets (Go).

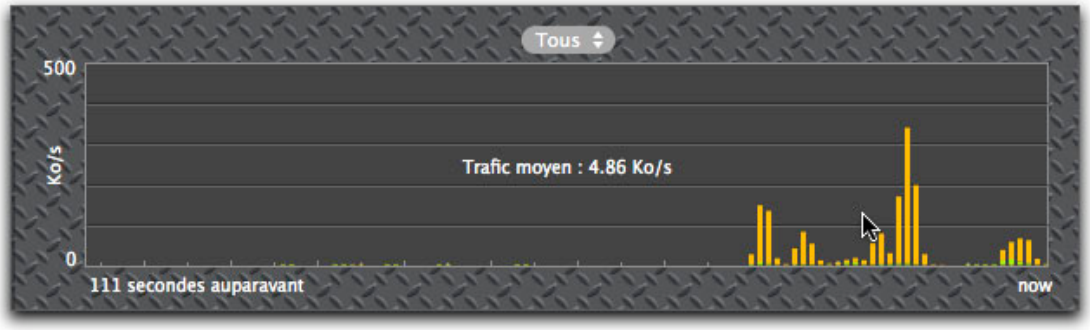
L'histogramme présente le trafic au fil du temps, où les barres le plus à droite retracent le présent, et celles à gauche le passé. Comme ci-dessus, les valeurs en orange représentent le trafic entrant, et les valeurs en vert le trafic sortant.

Cet histogramme a une échelle dynamique, variant selon la quantité de trafic. Dans l'exemple ci-dessus, la bande passante varie de 0 à environ 600 kilooctets par seconde, donc le graphe va jusqu'à 1000 kilooctets par seconde, comme on peut voir dans la légende sur la gauche. Dans le second exemple, ci-dessous, le trafic est très faible, il atteint seulement 4 kilooctets par seconde. Le graphe s'arrête donc à 5 kilooctets par seconde.

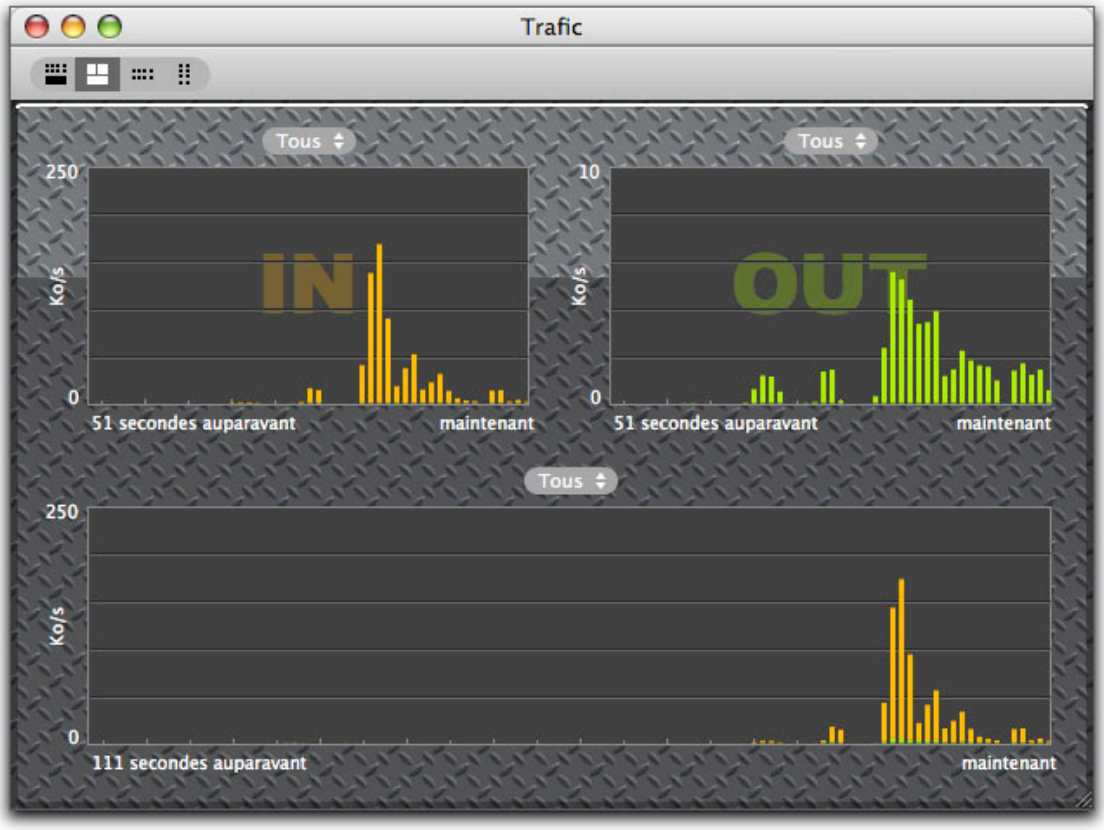
Par défaut, l'histogramme enregistre l'activité remontant à 111 secondes. Vous pouvez augmenter cette période en élargissant la fenêtre, soit en cliquant sur le bouton de "croissance" vert de Mac OS X dans le coin supérieur gauche, soit en cliquant et en faisant glisser le coin inférieur droit de la fenêtre. La période maximale est déterminée par la taille de votre écran, ou par votre choix de n'afficher qu'une section du temps à la fois.



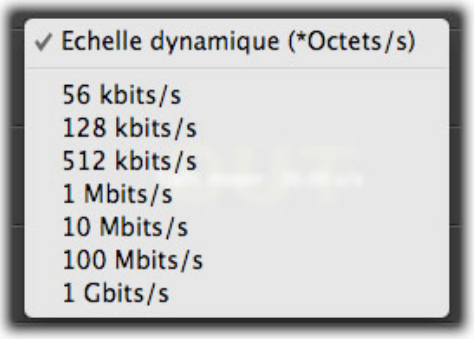
Si vous placez le curseur sur un histogramme, un texte apparaît, indiquant le débit moyen de données en cours, qui est mis à jour à chaque seconde.



Le second bouton affiche le trafic en trois histogrammes, présentant respectivement le trafic entrant, sortant et total.

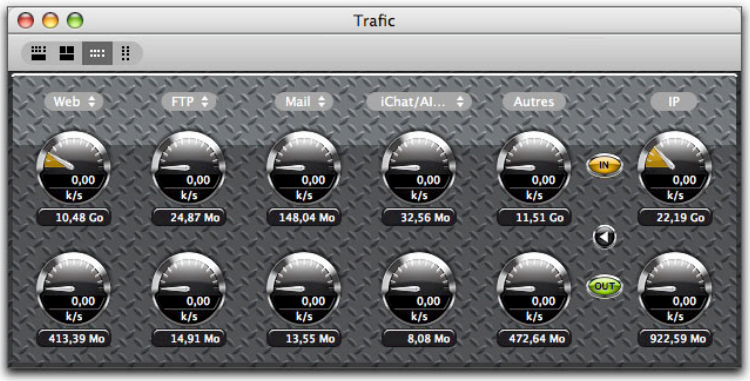


Ce mode d'affichage dispose d'une fonctionnalité spéciale qui laisse le choix de l'échelle pour les graphes In et Out en déplaçant la souris sur l'un d'eux, puis en cliquant tout en maintenant la touche Ctrl enfoncée. Un menu déroulant propose plusieurs options.



Cela permet de choisir la bande passante maximale et d'afficher des histogrammes à l'échelle adéquate. Choisissez Échelle dynamique, si vous voulez que l'échelle de l'histogramme varie selon la bande passante des données, comme décrit plus haut.

Le troisième bouton affiche le trafic en deux séries de compteurs à l'horizontale, sans histogramme. Le quatrième bouton affiche les mêmes compteurs, à la verticale (pas d'illustration).



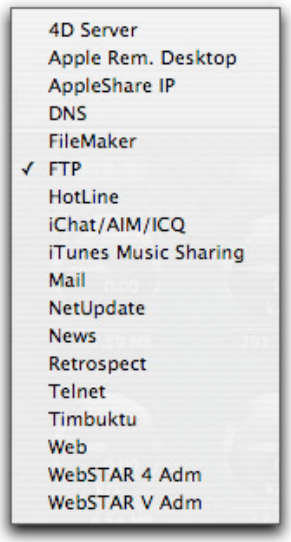
Les trois affichages avec compteurs disposent d'un bouton de remise à zéro. En cliquant sur ce bouton, les trafics cumulés des compteurs sont remis à zéro.

Choix du type de données de trafic

Dans chaque mode d'affichage, vous choisissez le type de trafic ; par défaut, les types suivants de données d'activité sont surveillés : Web, FTP, Mail, iChat/AIM. Le cinquième compteur indique tous les autres trafics et le sixième indique le trafic total.

Pour les quatre premières paires de compteurs, vous avez le choix du type de données enregistrées, en cliquant sur l'indicateur au-dessus de l'un des compteurs.

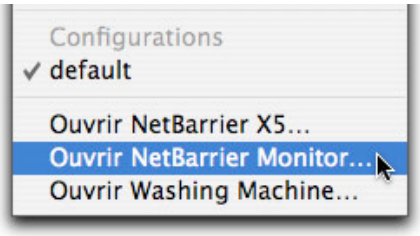
Le menu déroulant propose plusieurs choix.



Vous pouvez ajouter ou supprimer des services à la liste via le panneau des Préférences de trafic : pour plus de détails, consulter **Préférences du trafic,** au chapitre 10.

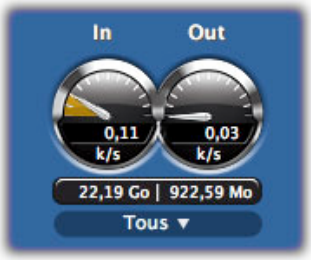
NetBarrier Monitor

Lors de l'installation de NetBarrier X5, une application appelée NetBarrier Monitor, est également installée dans le dossier Applications. Vous pouvez lancer ce programme en double-cliquant sur son icône, ou via le menu Intego (consulter **Menu Intego**).



L'application NetBarrier Monitor fournit une petite fenêtre flottante, qui permet d'avoir constamment un oeil sur l'activité réseau, sans devoir afficher toute la palette des compteurs d'activité de NetBarrier X5.

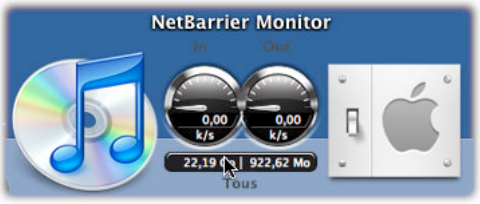
Quand vous ouvrez NetBarrier Monitor, sa fenêtre de compteurs d'activité s'affiche dans le coin inférieur droit de l'écran. Vous pouvez déplacer NetBarrier Monitor en cliquant dessus et en la faisant glisser vers l'endroit choisi sur l'écran.



Par défaut, NetBarrier Monitor affiche le trafic réseau total pour tous les services. Comme pour la section Trafic du programme principal NetBarrier X5, vous pouvez modifier le type de trafic affiché, en cliquant sur Tous au bas de la fenêtre de NetBarrier Monitor et en sélectionnant un service dans le menu déroulant.

En maintenant la touche Ctrl enfoncée et en cliquant sur cette fenêtre, un menu déroulant propose deux options.

Avec Afficher dans le Dock, la fenêtre de NetBarrier Monitor se ferme, l'icône du programme dans le Dock est modifiée et intègre les compteurs d'activité, mis à jour en temps réel.



L'activité réseau apparaît également dans l'icône de NetBarrier Monitor qui s'affiche quand vous basculez entre les applications en tapant sur Commande-Tab.

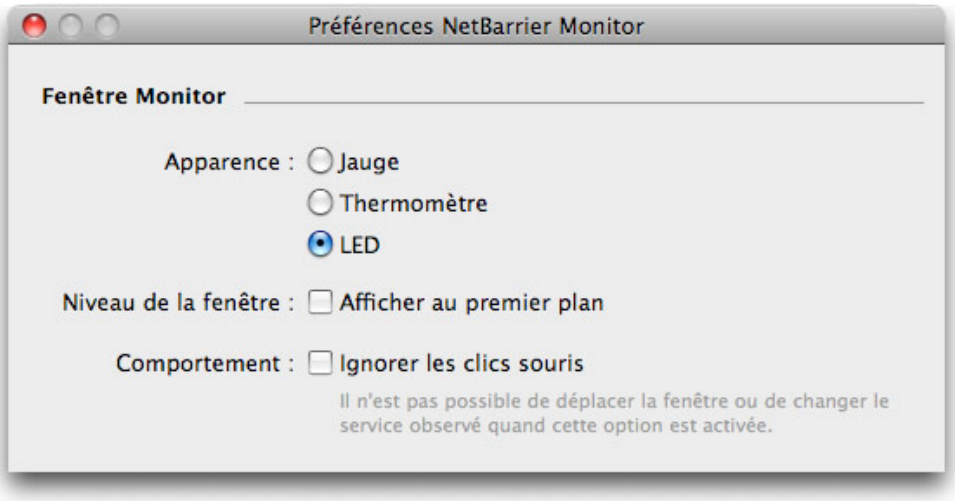
Pour revenir à la fenêtre de NetBarrier Monitor, maintenez la touche Ctrl enfoncée, cliquez sur l'icône de NetBarrier Monitor dans le Dock et sélectionnez Afficher dans une fenêtre.

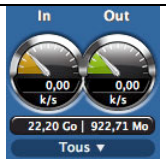
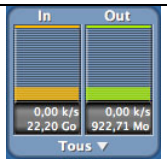
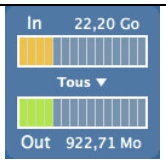
Quand NetBarrier Monitor s'affiche dans le Dock, vous pouvez modifier son affichage en maintenant la touche Ctrl enfoncée, cliquant sur son icône dans le Dock et sélectionnant un service différent dans son menu.

La sélection Maintenir dans le Dock place l'icône de NetBarrier Monitor en permanence dans le Dock, même quand le programme ne fonctionne pas, et il suffit de cliquer sur cette icône pour l'ouvrir. Avec la sélection Ouvrir avec la session, le programme démarre chaque fois que vous lancez une session utilisateur sur votre Mac.

Préférences de NetBarrier Monitor

Plusieurs réglages de préférences concernent le comportement de NetBarrier Monitor. Pour les régler, allez à NetBarrier Monitor > Préférences ou appuyez sur Commande-virgule, NetBarrier Monitor étant en fonctionnement.

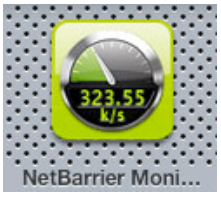


Apparence	Jauge :  Thermomètre :  LED : 
Niveau de la fenêtre	En cochant "Afficher au premier plan", NetBarrier Monitor apparaît toujours au premier plan, au-dessus des autres applications.
Comportement	En cochant "Ignorer les clics souris", vous ne pouvez pas déplacer la fenêtre de NetBarrier Monitor ni modifier le service supervisé.

Widget NetBarrier Monitor

NetBarrier X5 installe le widget NetBarrier Monitor, qui se charge dans le Dashboard de Mac OS X (uniquement Mac OS X 10.4 Tiger et ultérieur) et affiche à tout moment l'activité réseau.

Pour afficher le widget NetBarrier Monitor, activez Dashboard. Cliquez sur le bouton + pour afficher tous les widgets disponibles sur l'ordinateur. Sélectionnez NetBarrier Monitor dans la liste. Son icône a l'aspect suivant :

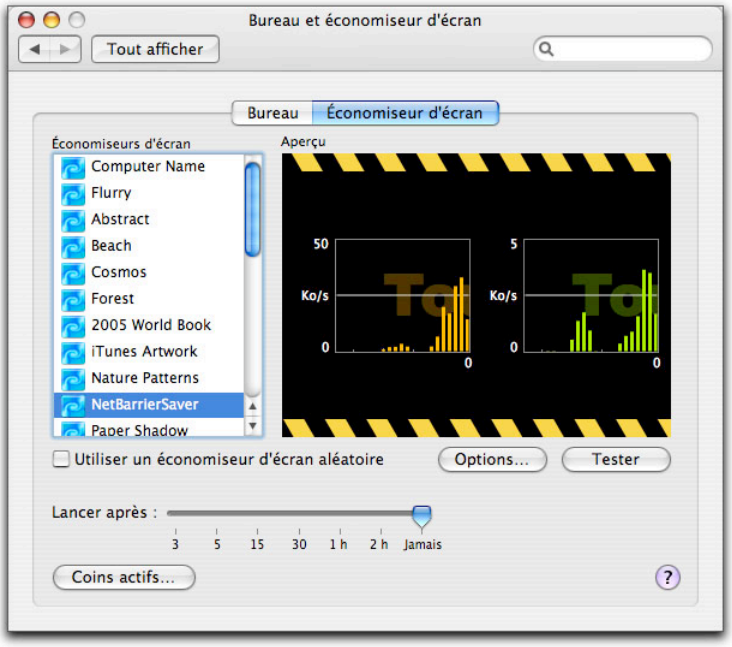


Par cette sélection, il est ajouté aux widgets actifs, et NetBarrier Monitor s'affiche chaque fois que vous basculez sur Dashboard. Comme pour l'application NetBarrier Monitor, vous pouvez déplacer la fenêtre ou modifier le type d'activité présenté.

Économiseur d’écran de supervision de NetBarrier X5

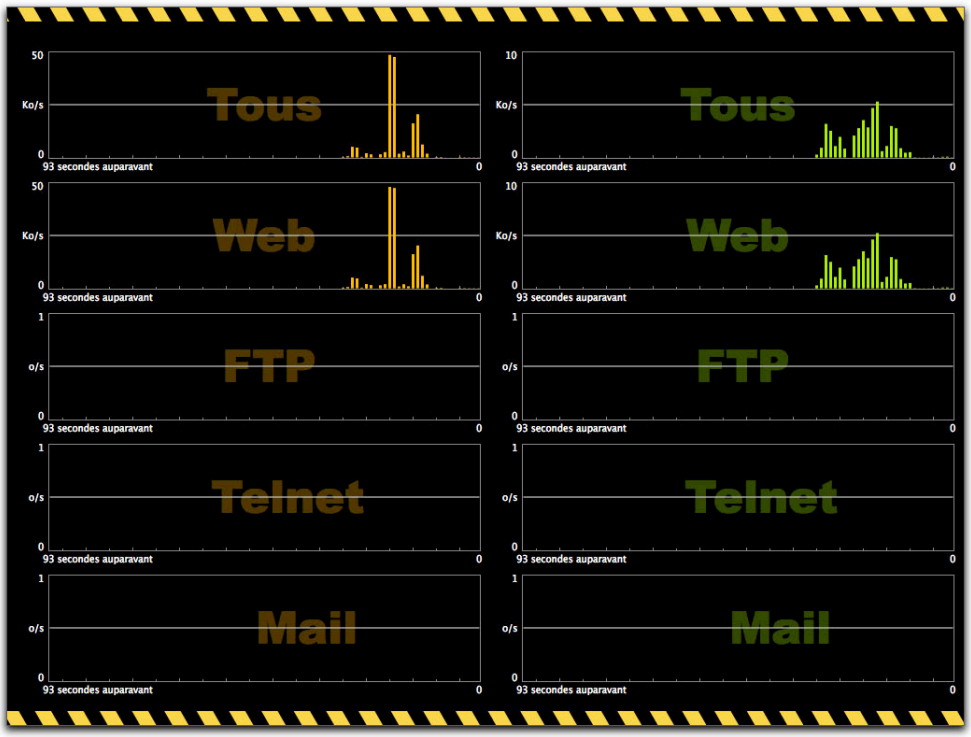
NetBarrier X5 installe un économiseur d’écran, qui propose une vue générale de l’activité réseau quand l'ordinateur est par ailleurs inactif. De plus, si le Macintosh fonctionne en serveur, cet économiseur d’écran peut servir à garder un oeil sur l’activité réseau.

Pour utiliser l’économiseur d’écran de NetBarrier X5, ouvrez les Préférences Système, dans le menu Apple, cliquez sur Bureau et économiseur d’écran, puis sur l’onglet Économiseur d’écran. Sélectionnez NetBarrierSaver dans la liste des économiseurs d’écran.



L'écran Aperçu présente seulement tous les trafics ; cependant, en fonctionnement réel, il présentera le trafic réparti par service. Cliquez sur Options... pour choisir l'ordre d'affichage des services.

Faites-les glisser selon l'ordre de votre choix. Le nombre de services affichés dépend de la résolution d'écran et du nombre d'écrans choisis : il faut lister d'abord ceux qui sont les plus importants.



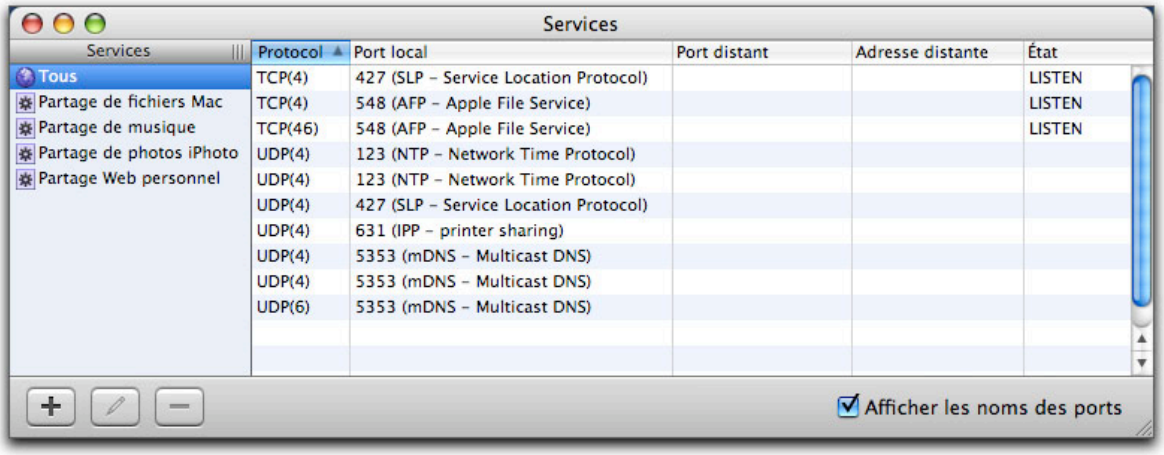
Pour en savoir plus sur les réglages d'économiseur d'écran, reportez-vous à l'Aide de Mac OS X.

Services

Le panneau Services liste tous les services actifs sur l'ordinateur qui sont accessibles à d'autres utilisateurs via le protocole Internet, tels qu'un serveur web, un serveur de courrier, etc.

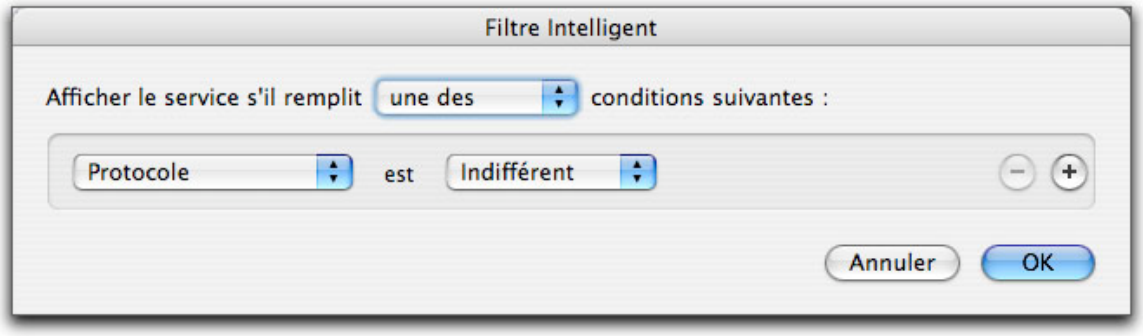
Pour afficher le panneau Services, cliquez sur l'icône de double-flèche dans le coin inférieur droit de l'interface principale de NetBarrier X5.

Pour chaque port utilisé, les informations suivantes sont présentées : le protocole (TCP ou UDP), le numéro de port local (selon le protocole représenté, s'il s'agit d'un protocole standard ; par exemple, le port 21 est HTTP), le numéro de port distant, l'adresse distante (adresse IP de la connexion à distance), et l'état de la connexion – par exemple, si la connexion est active ou juste en veille. Pour obtenir les noms des ports, en plus de leurs numéros, cochez la case **Afficher les noms des ports**, dans le coin inférieur droit, comme indiqué ici.



Comme la liste des ports utilisés par tous les services peut être longue, NetBarrier X5 propose des filtres permettant de visualiser les ports utilisés par des services spécifiques. Vous avez le choix entre Partage de fichiers Mac, Partage de musique, Partage de photos, ou Partage Web personnel, et vous pouvez créer vos propres filtres.

Pour cela, cliquez sur le bouton + en bas à gauche du panneau. La fenêtre Filtre Intelligent apparaît :



Par le premier menu déroulant, vous déterminez si vous voulez que le filtre corresponde à l'une ou à l'ensemble des conditions.

Par le second menu déroulant, précisez le type d'information sur lequel le filtre va agir. Les choix sont identiques à ceux des colonnes du panneau Services : Protocole, Port local, Port distant, Adresse distante et État. Après avoir choisi, vous pouvez préciser les détails du filtre. Dans cet exemple, nous allons seulement lister les services dont le port local se trouve dans un intervalle donné.

Pour ajouter des conditions supplémentaires, cliquez sur le bouton + à droite de la liste ; en cliquant sur le bouton – à côté d'une condition, vous la supprimez. Vous pouvez également modifier les conditions des filtres en changeant leurs options du menu déroulant ou en tapant des données nouvelles dans les champs de données.

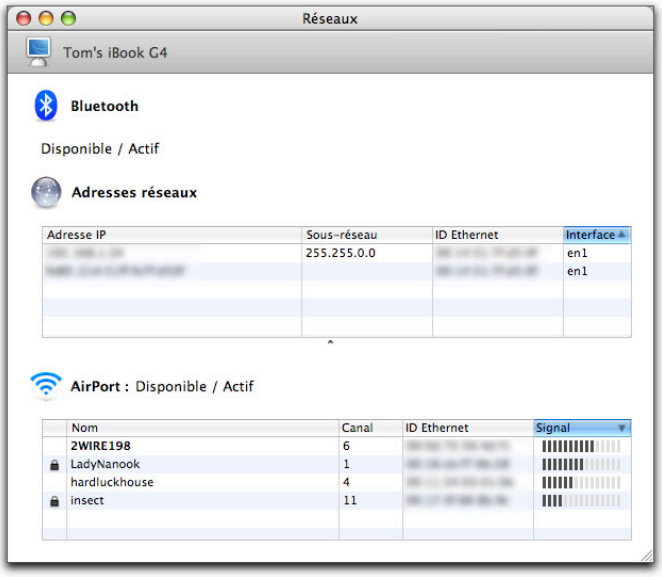
Quand vous avez terminé, cliquez sur OK pour enregistrer le filtre, puis saisissez le nom du filtre dans la liste des Services. Cliquez sur le filtre, à tout moment, dans la liste pour voir les services de réseau correspondant à vos conditions.

Réseaux

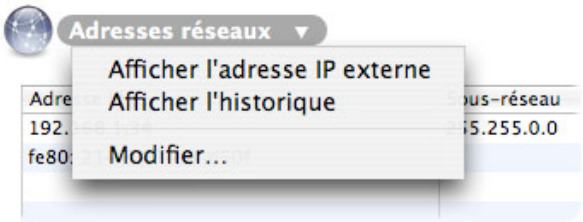
Le panneau Réseaux rassemble des informations utiles concernant l'ordinateur, sa configuration réseau, ainsi que les réseaux locaux qui lui sont disponibles. Pour afficher le panneau Réseaux, cliquez sur l'icône de radio dans le coin inférieur droit de l'interface principale de NetBarrier X5.

Le panneau Réseaux contient :

Le nom de votre Mac	Indiqué dans la barre grisée en haut : dans l'exemple ci-dessous, il s'agit de "Tom's iBook G4". C'est le nom que votre ordinateur indique à tout utilisateur qui le recherche sur un réseau. Vous pouvez le modifier dans le panneau Partage des Préférences Système.
Bluetooth	Indique si le matériel Bluetooth est disponible et actif.
Adresses réseaux	Toutes les adresses IP qui sont actives sur votre Mac. Si vous avez plusieurs adaptateurs de réseau avec des adresses différentes, ou si vous utilisez plusieurs serveurs, il apparaît plus d'une adresse. Sont également indiqués les sous-réseaux, les ID Ethernet et les interfaces (au format de nom BSD).
AirPort	Disponibilité et état d'une carte de réseau sans fil. Si votre carte AirPort est disponible et active, le tableau indique les réseaux sans fil disponibles, leurs Canaux, leurs ID Ethernet, et le niveau de signal en fonction de votre position actuelle. (La force du signal est proportionnelle au nombre de barres foncées.) Les réseaux sans fil qui nécessitent un mot de passe ou une autre clé d'accès sont accompagnés d'une petite icône de cadenas. Ceux sans cadenas ne disposent pas de mot de passe de réseau ; ils peuvent, cependant, être protégés par d'autres moyens, tels que l'authentification web. Si vous êtes connecté à un réseau sans fil, il est affiché en caractères gras.



Plusieurs fonctions et options sont disponibles pour le panneau Réseaux, en cliquant sur l'étiquette "Adresses réseaux".

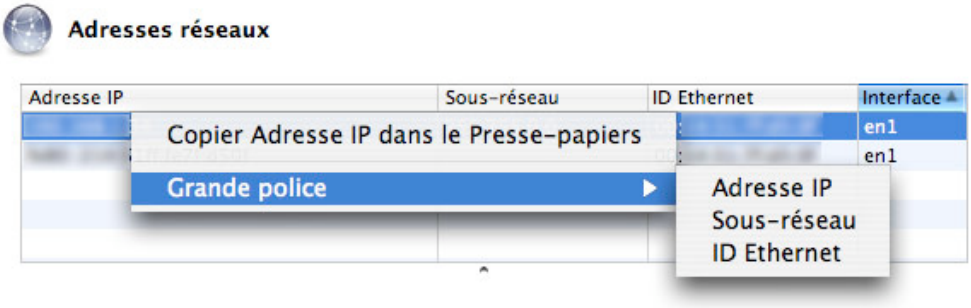


Il s'agit des options suivantes :

Afficher l'adresse IP externe	Pour présenter, en gros caractères, l'adresse IP externe utilisée par l'ordinateur pour la connexion à Internet ou à d'autres réseaux. Cette adresse diffère de celle que NetBarrier X5 affiche dans ce panneau si vous avez un routeur, ou un modem câble ou DSL. Cliquez n'importe où sur l'écran pour faire disparaître l'information.
Afficher l'historique	Une liste indique les différentes adresses IP attribuées à votre Mac par votre fournisseur d'accès Internet, si l'adressage est dynamique. Cependant, si vous avez un routeur, ou un modem câble, seule est indiquée l'adresse IP que l'ordinateur utilise en interne.
Modifier...	Pour ouvrir le panneau Réseau des Préférences Système de Mac OS X. Vous pouvez modifier les adresses réseau ou le nom de l'ordinateur dans ce

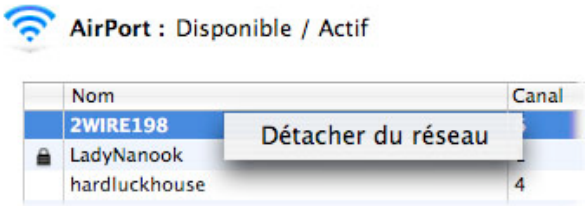
	panneau. Pour en savoir plus sur les réglages de Réseau, reportez-vous à l'Aide de Mac OS X.

D'autres options sont disponibles pour des entrées individuelles dans la zone "Adresses réseaux". Pour les révéler, maintenez la touche Ctrl enfoncée tout en cliquant sur l'entrée concernée. Un menu contextuel apparaît.



Copier Adresse IP dans le Presse-papiers	Pour placer l'information, en texte simple, sur le Presse-papiers de Mac OS X, d'où vous pouvez la coller dans d'autres applications.
Grande police	Pour afficher en plein écran un des trois types d'informations liées à l'entrée concernée : adresse IP, sous-réseau ou ID Ethernet. En cliquant ailleurs sur l'écran, on fait disparaître cet affichage en gros caractères.

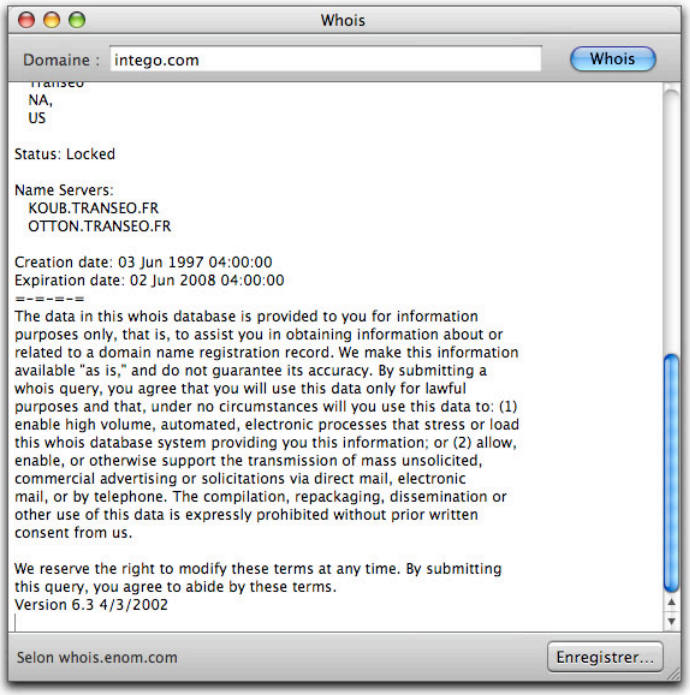
Enfin, en Ctrl-cliquant sur les entrées dans la section AirPort, un menu contextuel permet de détacher votre Mac du réseau auquel il est actuellement attaché.



Whois

NetBarrier X5 sait rechercher les noms de domaine et les adresses IP sur Internet grâce à l'outil intégré Whois, que vous lancez en cliquant sur le bouton **?**, en bas à droite de l'écran.

Entrez un nom de domaine ou une adresse IP dans le champ Domaine, puis cliquez sur le bouton Whois ou appuyez sur la touche Entrer. Le large champ de texte présente les informations relatives au domaine, récupérées sur des serveurs d'infos accessibles au public. Vous pouvez enregistrer ces informations dans un fichier texte, en cliquant sur le bouton Enregistrer….



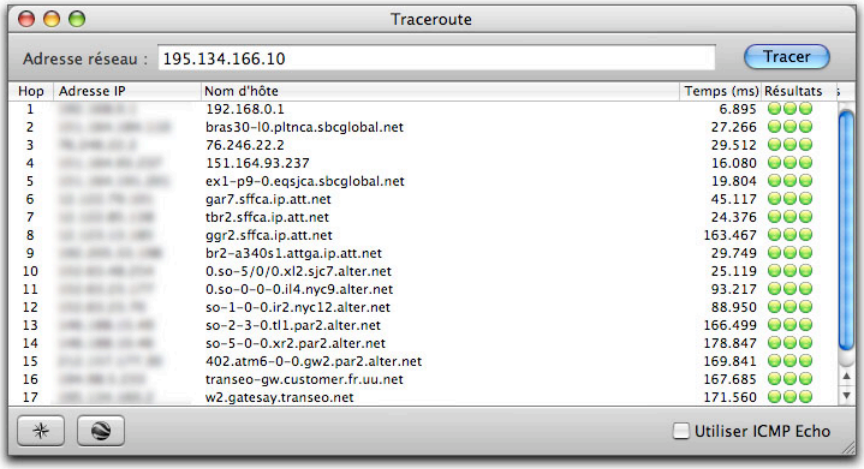
Suite à la réception de ces informations, le nom du serveur d'origine est précisé dans la barre grisée au bas du panneau. NetBarrier X5 inclut cinq serveurs Whois par défaut, et vous pouvez compléter ou modifier la liste. Pour savoir comment ajouter des serveurs Whois, reportez-vous au chapitre 10, **Préférences et configurations**.

Traceroute

Quand vous échangez des données via Internet ou d'autres réseaux, ces données sont transmises en paquets d'un hôte à un autre, en faisant des dizaines de sauts intermédiaires, jusqu'à atteindre leur destination. La fonction Traceroute de NetBarrier X5 peut aider à visualiser exactement le chemin pris par les données jusqu'à leur destination ; c'est particulièrement utile en cas de problèmes lors de l'accès à un hôte spécifique, pour pouvoir localiser le point de blocage. Dans ce cas, cela correspond souvent au mauvais fonctionnement d'un hôte ou d'un routeur clé.

Lancez l'outil Traceroute de NetBarrier en cliquant sur l'icône de flèche en Y, dans le coin inférieur droit du panneau.

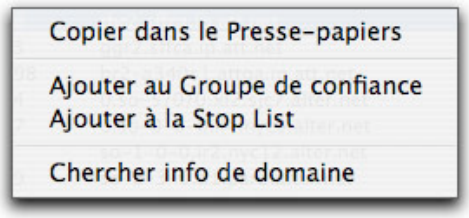
Pour lancer une Traceroute, entrez une adresse IP ou un nom de domaine dans le champ Adresse réseau, puis cliquez sur Tracer ou appuyez sur la touche Entrer. Si vous entrez un nom de domaine, NetBarrier X5 le résout et affiche l'adresse IP. Si vous cochez Utiliser ICMP Echo, la Traceroute envoie des demandes ICMP au lieu des demandes UDP ; dans certains cas, cela peut être plus efficace.



La fenêtre de Traceroute montre tous les sauts entre votre ordinateur et l'hôte final. Pour chaque saut, NetBarrier X5 affiche son numéro, l'adresse IP, le nom de l'hôte, le temps de réponse en

millisecondes, et le nombre de pings qui ont réussi (pastilles vertes) ou échoué (pastilles rouges). NetBarrier X5 envoie trois pings pour chaque saut ou pour chaque étape. Notez que, si votre réseau est équipé d'un routeur, celui-ci peut ne pas répondre à la demande de Traceroute, et il peut afficher comme si les demandes avaient échoué. Cela n'empêche pas l'exécution du reste de la Traceroute.

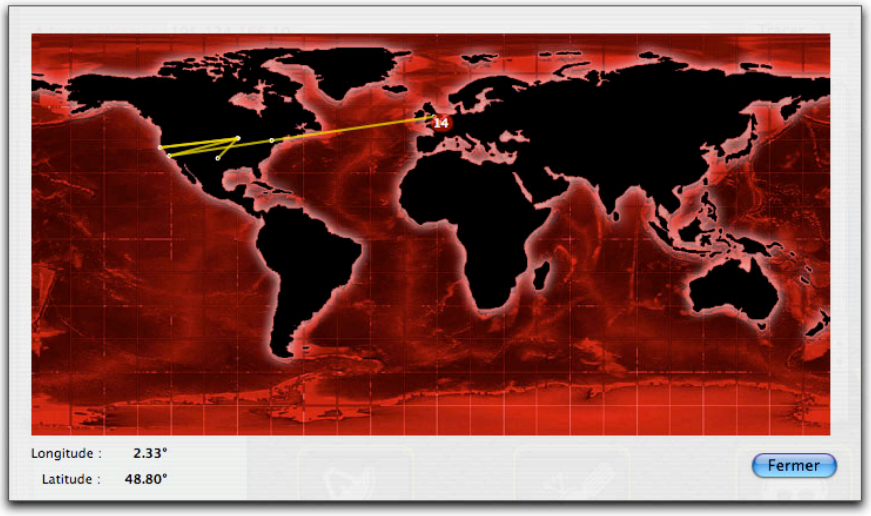
A la fin de la Traceroute, vous pouvez Ctrl-cliquer sur une ligne et un menu contextuel apparaît.



Copier dans le Presse-papiers	Pour placer l'information, en texte simple, sur le Presse-papiers de Mac OS X, d'où vous pouvez la coller dans d'autres applications.
Ajouter au Groupe de confiance	Pour l'ajout permanent de cette adresse IP au Groupe de confiance, ce qui permet les connexions futures, indépendamment des réglages de l'Antivandale. Cependant, le Firewall de NetBarrier X5 affecte toujours les communications venant de cette adresse IP.
Ajouter à la Stop List	Pour l'ajout permanent de cette adresse IP à la Stop List, ce qui bloque les connexions futures, indépendamment des réglages de l'Antivandale. Cependant, le Firewall de NetBarrier X5 affecte toujours les communications venant de cette adresse IP.
Chercher info de domaine	Pour lancer la fenêtre Whois de NetBarrier X5 et faire des recherches sur l'adresse IP sélectionnée. Consulter **Whois** pour plus d'infos.

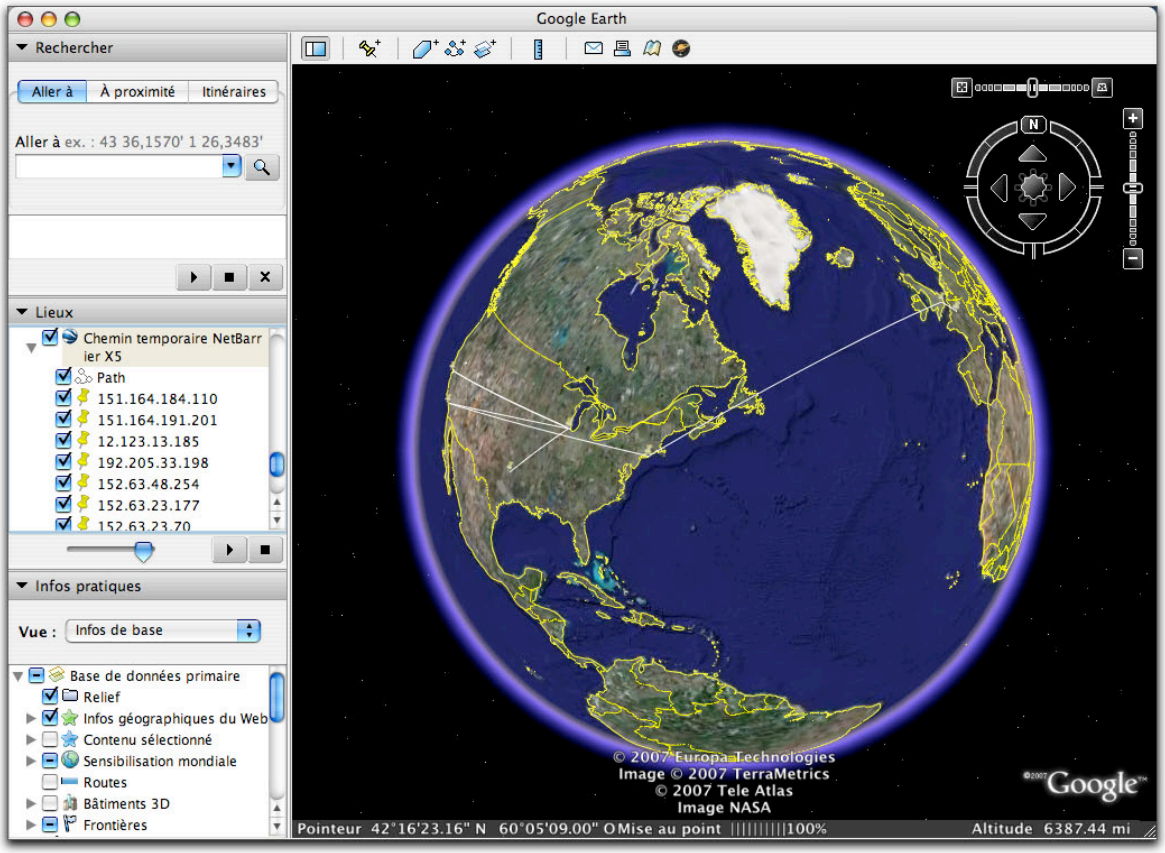
Vous obtenez un affichage cartographique du chemin pris par les données, en cliquant sur le bouton de rosace en bas à gauche.

Une mappemonde présente les lignes connectant chaque saut, et les numéros indiquant leur position sur le chemin.



Si vous cliquez sur le bouton Google Earth, en bas à gauche, le logiciel Google Earth ayant été installé sur votre Mac, NetBarrier X5 va ouvrir Google Earth et zoomer sur l'emplacement géographique précis de l'adresse IP. Note : cela ne fonctionne pas pour les adresses sur votre réseau local, et cela ne fonctionnera pas avec toutes les adresses IP.

Le chemin et les sauts apparaissent dans “Chemin temporaire NetBarrier X5” sous la section Lieux de Google Earth, et ils s'affichent automatiquement. Pour plus d'informations concernant Google Earth, téléchargeable gratuitement, visitez le site http://earth.google.com.


Google Earth
Rechercher
Aller à
À proximité
Itinéraires
Aller à ex. : 43 36,1570' 1 26,3483'
Lieux
Chemin temporaire NetBarrier X5
Path
151.164.184.110
151.164.191.201
12.123.13.185
192.205.33.198
152.63.48.254
152.63.23.177
152.63.23.70
Infos pratiques
Vue :
Infos de base
Base de données primaire
Relief
Infos géographiques du Web
Contenu sélectionné
Sensibilisation mondiale
Routes
Bâtiments 3D
Frontières
© 2007 Europa Technologies
Image © 2007 TerraMetrics
© 2007 Tele Atlas
Image NASA
Google
Pointeur 42°16'23.16" N 60°05'09.00" O
Mise au point
100%
Altitude 6387.44 mi

NetUpdate

NetUpdate est une application que les programmes Intego utilisent pour vérifier la présence éventuelle d'une mise à jour. Cette application est installée en même temps que NetBarrier X5 ou les autre logiciels d'Intego. Elle vérifie simultanément les mises à jour de tous ces programmes, et télécharge et installe celles relatives aux programmes installés sur votre ordinateur.

NetUpdate vérifie périodiquement les mises à jour, ou vous pouvez la forcer à vérifier immédiatement, en cliquant sur le bouton **Vérifier...** en haut à gauche dans l'écran Aperçu de NetBarrier X5.

Pour en savoir plus sur l'utilisation de NetUpdate, reportez-vous au Manuel de Démarrage Intego.

9 - Comprendre les alertes

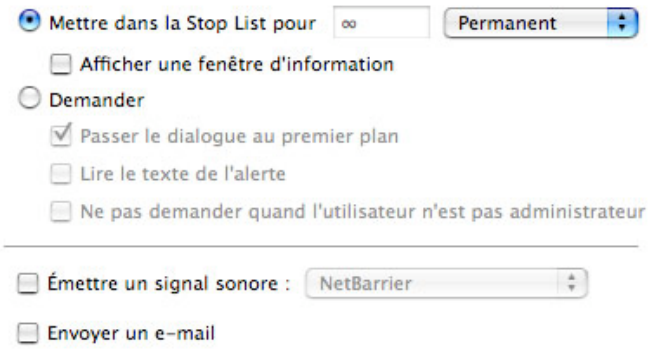
NetBarrier X5 surveille constamment l'activité réseau de l'ordinateur, sur Internet ou sur un réseau local, et il recherche des types spécifiques de données indiquant une intrusion ou une attaque. Si NetBarrier X5 trouve des données suspectes, il affiche une alerte et demande si vous souhaitez laisser passer ces données ou les refuser.

Réglages d'alertes

Les alertes peuvent apparaître en réaction aux réglages dans les sections suivantes :

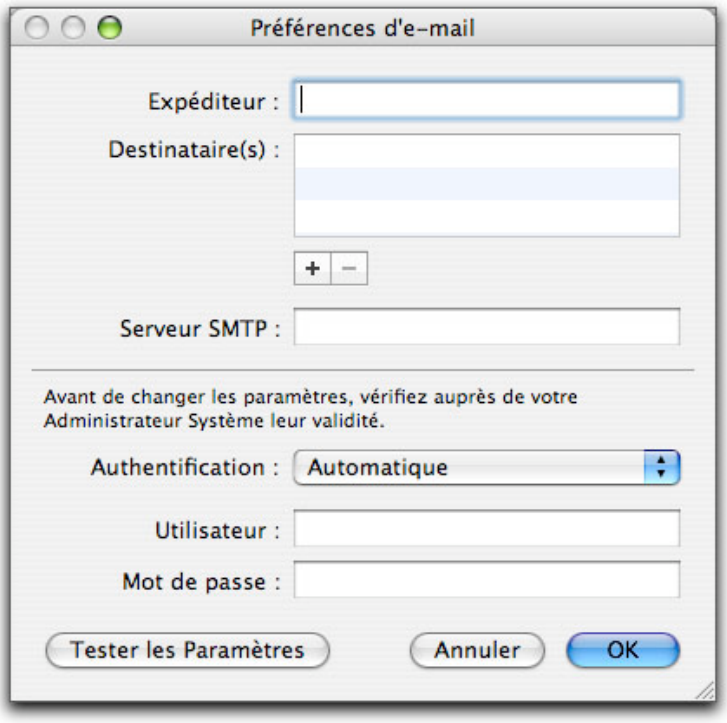
- Troyens
- Données
- Surf
- Politiques
- Anti-Spyware

Les réglages pour ces alertes se retrouvent en plusieurs endroits dans NetBarrier X5, comme cela est décrit dans les sections applicables de ce manuel. Pour mieux comprendre ces réglages, nous allons les aborder comme ils apparaissent dans la section Politiques.



Mettre dans la Stop List pour	Si ce bouton radio est activé, la connexion est automatiquement coupée en cas d'alerte et l'adresse IP attaquante est immédiatement reprise dans la Stop List (consulter **Stop List et Groupe de confiance**.) Le champ à droite de ce bouton permet de spécifier la durée par défaut du maintien de l'adresse IP dans la Stop List. Vous indiquez la durée de votre choix, en secondes, minutes, heures ou jours, ou vous placez l'intrus en permanence dans la Stop List.
Demander	Si ce bouton radio est activé, NetBarrier X5 présente un dialogue d'alerte demandant le mode d'action. En cas d'apparition d'une alerte, il indique la durée par défaut de séjour dans la Stop List, et cette durée peut être modifiée dans l'onglet Politique selon le type d'attaque. En complément, vous disposez de trois options : • **Passer le dialogue au premier plan** : Chaque alerte éventuelle vient automatiquement au premier plan. Sinon, elle reste en arrière-plan. Si vous n'intervenez pas dans les 90 secondes qui suivent, l'alerte se ferme automatiquement et la connexion est refusée. • **Lire le texte de l'alerte** : NetBarrier X5 utilise la synthèse vocale de Mac OS X pour lire le texte de l'alerte. • **Ne pas demander quand l'utilisateur n'est pas administrateur** : NetBarrier X5 propose seulement les options ci-dessus si l'utilisateur Mac OS X a des privilèges d'administrateur. Sinon, il place automatiquement l'hôte attaquant dans la Stop List.
Emettre un signal sonore	NetBarrier X5 émet le signal sonore de votre choix à chaque alerte. Vous pouvez le choisir dans le menu déroulant situé à droite du bouton.
Envoyer un e-mail	NetBarrier X5 envoie un courrier électronique, dans un délai de 30 secondes, à l'adresse configurée dans le panneau Options (voir ci-après). (NetBarrier X5 attend pour voir s'il y a d'autres tentatives d'intrusion, plutôt que d'envoyer un courrier électronique à chaque alerte.)

Pour recevoir les notifications d'alerte par message électronique, vous devez en configurer les réglages. Dans la section Politiques, vous cliquez sur Options, puis sur le bouton Configurer….



Vous devez saisir les adresses de l'expéditeur et du (ou des) destinataire(s), ainsi que le serveur SMTP. Puis, vous devez entrer un nom d'utilisateur et un mot de passe que votre serveur de messagerie va accepter. Plusieurs destinataires peuvent recevoir les messages. Pour ajouter un destinataire, cliquez sur le bouton +. Pour éliminer un destinataire, cliquez sur le bouton -.

Exemples d'alertes

L'exemple ci-dessous est une alerte quand le bouton radio "Mettre dans la Stop List" est activé et quand la case **Afficher une fenêtre d'information** est cochée.

Vous constatez qu'il n'y a pas d'options, mais une simple notification. Si la case **Afficher une fenêtre d'information** n'avait pas été cochée, vous n'auriez rien vu et NetBarrier X5 aurait ajouté, en silence, l'adresse IP à la Stop List.

L'exemple ci-dessous est une alerte quand le bouton radio Demander est activé et quand la case **Passer le dialogue au premier plan** est cochée.

La première ligne indique la raison de l'alerte. L'hôte (ici, en estompé) est indiqué par une adresse IP, mais vous pouvez trouver le nom de domaine associé (le cas échéant) en cliquant sur l'icône **?**. Nous avons déjà cliqué sur le triangle pour présenter Plus d'informations, ce qui donne plus de détails et d'instructions.

Les deux boutons à droite permettent de décider de la suite à donner à cette alerte.

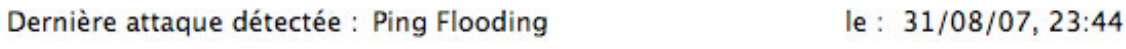
Stop List	La Stop List est la réponse par défaut à toutes les alertes. Si vous cliquez sur ce bouton, ou si vous appuyez sur la touche Entrer ou Retour, les données reçues sont refusées et l'intrusion est bloquée. Le paquet est alors perdu : c'est comme si les données n'avaient jamais été reçues. Si le paquet suspect fait partie d'un fichier, ce dernier n'arrivera pas à destination. S'il s'agit une commande, elle n'aura aucune chance d'être exécutée, puisqu'elle n'atteindra pas sa cible. En complément, l'adresse IP à l'origine de cette alerte sera automatiquement ajoutée à la Stop List, où elle sera conservée pendant la durée par défaut qui a été définie. Vous pouvez modifier cette durée dans le menu déroulant.
Ignorer	Si vous cliquez sur ce bouton, vous autorisez l'envoi des données. La transmission des données continuera comme d'habitude, à moins que NetBarrier X5 ne détecte une nouvelle tentative d'intrusion, auquel cas une autre alerte apparaît.

Enfin, voici l'exemple d'une alerte se produisant quand une application essaie d'atteindre l'Internet en violation de règles Anti-Spyware.

Compteur d’attaques

NetBarrier X5 enregistre le nombre d’attaques contre lesquelles il a protégé l’ordinateur et affiche ce nombre en bas du panneau Politique de l’Antivandale. Il indique le type de la dernière attaquée bloquée, ainsi que la date et l’heure. D'abord, le nombre d'attaques apparaît :

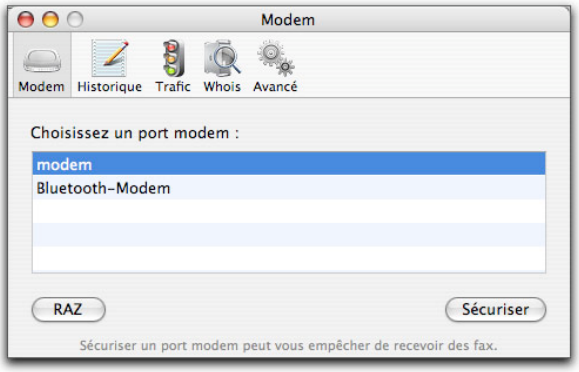
Au bout de quelques secondes, NetBarrier X5 indique les informations relatives à l'attaque la plus récente :



Pour réinitialiser le compteur, cliquez sur le bouton de remise à zéro.

10 - Préférences et configurations

Les préférences concernant plusieurs fonctions du logiciel sont disponibles dans l'écran des préférences de NetBarrier. Pour voir cet écran, choisissez NetBarrier X5 > Préférences..., ou appuyez sur Commande-virgule. Une fenêtre apparaît, où la première des cinq icônes, Modem, est sélectionnée.

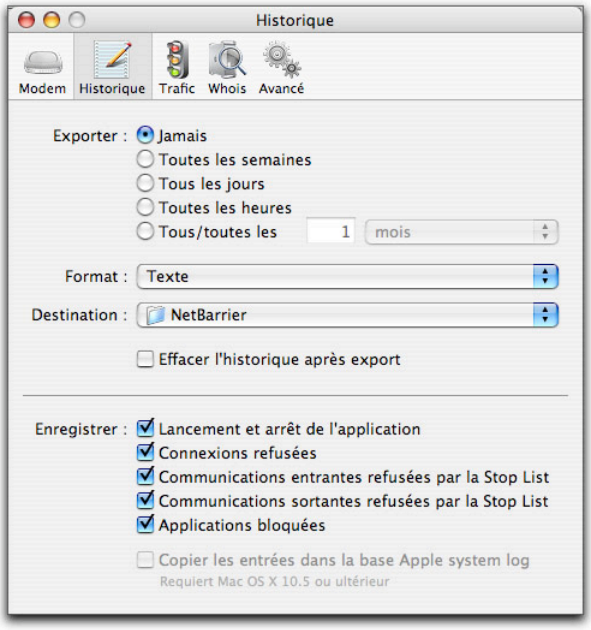


Préférences du modem

Cette option assure une sécurité totale à votre modem, en bloquant les appels entrants. Pour cela, cliquez sur le bouton **Modem** dans l'écran des préférences. En le sécurisant, il est possible que votre modem ne puisse plus répondre aux appels. En cliquant sur le bouton Sécuriser, vous indiquez à NetBarrier X5 de ne pas accepter d'appels entrants ; cependant, vous pouvez toujours passer des appels sortants. Pour ramener le modem à son état normal, non sécurisé, cliquez sur le bouton **RAZ**.

Préférences de l'historique

NetBarrier X5 sait exporter l'historique à intervalles réguliers. Pour cela, cliquez sur le bouton **Historique** dans l'écran des préférences.



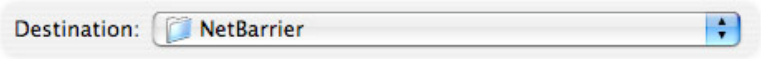
Votre premier choix concerne le mode d'export de l'historique. Si le bouton radio **Toutes les semaines** est activé, les exports se produisent chaque dimanche soir, à minuit ; pour **Tous les jours**, ils se produisent à minuit ; pour **Toutes les heures**, ils se produisent à chaque passage d'heure. La sélection personnalisée **Tous/toutes les** permet de préciser un multiple de ces moments, par exemple, une fois toutes les deux semaines. (Cette sélection **Tous/toutes les** permet également d'exporter mensuellement, à minuit le premier jour du mois.)

Si l'ordinateur est éteint au moment de l'export planifié, l'export se produit dès l'allumage suivant.

Les historiques sont exportables selon six formats ; pour sélectionner le format d'export, cliquez sur le menu déroulant Format.

Pour en savoir plus, reportez-vous au paragraphe **Export de l'historique**.

Vous pouvez choisir le dossier où sont enregistrés les fichiers d'export de l'historique. Par défaut, ils sont enregistrés dans le dossier /Library/Logs/NetBarrier. Si vous décidez d'un autre dossier, sélectionnez le bouton Autre... dans le menu déroulant et naviguez jusqu'à ce que vous l'ayez trouvé. Puis cliquez sur Choisir pour activer ce dossier.



NetBarrier X5 utilise deux historiques. Il existe un historique rotatif, contenant un maximum de 4096 lignes, que vous voyez dans le panneau Historique de NetBarrier X5. Si les exports automatiques sont activés, un second historique stocke toutes les entrées. Si vous souhaitez conserver des historiques complets de toute l'activité, nous vous conseillons d'activer les exports périodiques. Ces historiques ne sont pas limités en taille (autre que l'espace disponible sur le disque dur). Si vous cochez "Effacer l'historique après export", les lignes de l'historique seront effacées, et chaque nouvel export ne contient que les lignes enregistrées depuis l'export précédent. Ce réglage ne concerne que les exports automatisés, et non pas les exports faits manuellement depuis la fenêtre de l'historique.

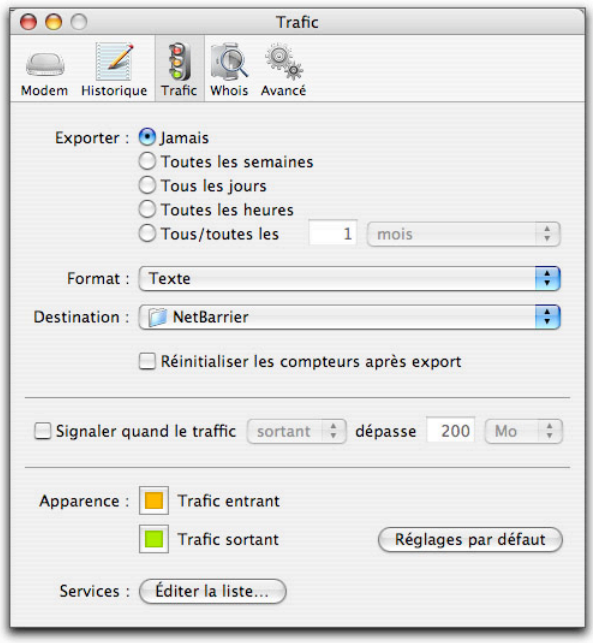
Vous avez le choix des éléments enregistrés dans les historiques, selon les cases à cocher au bas du panneau des préférences de l'historique. Les options sont les suivantes :

Lancement et arrêt de l'application	Activité générale de NetBarrier X5, telle que le démarrage ou l'arrêt.
Connexions refusées	Tentatives d'atteindre votre Mac qui ont été bloquées pour cause de violation de règles que vous avez établies dans NetBarrier X5.
Communications entrantes refusées par la Stop List	Tentatives d'envoi, à votre Mac, de données venant d'hôtes se trouvant dans la Stop List.
Communications sortantes refusées par la Stop List	Tentatives d'envoi, depuis votre Mac, de données destinées à des hôtes se trouvant dans la Stop List.
Applications bloquées	Cas où l'Anti-Spyware de NetBarrier X5 a empêché la communication entre une application et le réseau.

La dernière case traite de **Copier les entrées dans la base Apple system log**. Si elle est cochée, les données de l'historique sont enregistrées dans un système d'historique unifié se trouvant dans Mac OS X 10.5 et ultérieur.

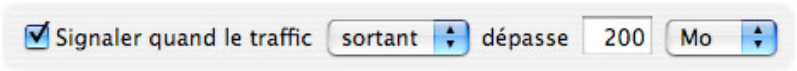
Préférences du trafic

Comme les préférences de l'historique, l'écran des préférences du trafic propose des options pour l'export des données à intervalles réguliers. Plusieurs options de gestion des données du trafic sont disponibles. Pour modifier ces réglages, cliquez sur le bouton Trafic dans l'écran des préférences.



En partie supérieure, vous contrôlez les exports périodiques et automatisés des données du trafic. Le fonctionnement est identique à celui des préférences de l'historique : voir ci-dessus pour plus de détails. Le seul réglage différent est la case **Réinitialiser les compteurs après export**, qui est similaire à la case **Effacer l'historique après export** pour les historiques. Cocher cette case est équivalent à cliquer sur le bouton de remise à zéro, pour réinitialiser le trafic total, suite aux exports automatisés. Pour en savoir plus sur les compteurs de trafic, consultez **Trafic.**

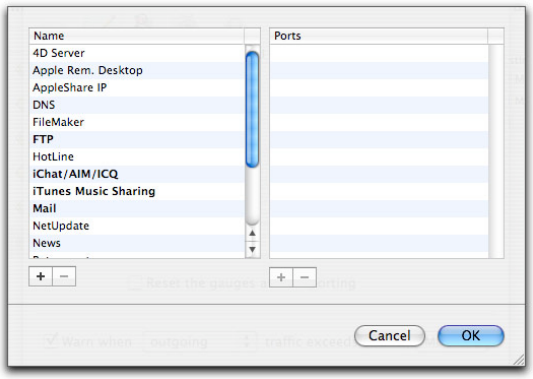
Les préférences du trafic de NetBarrier X5 incluent un réglage permettant de surveiller la quantité de données entrant ou sortant de votre ordinateur. C'est utile si votre compte d'accès Internet a des limitations de trafic entrant ou sortant.



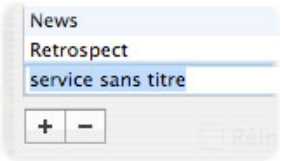
Si vous cochez cette option, NetBarrier X5 affiche un avertissement quand le trafic dépasse le seuil choisi. L'avertissement peut s'appliquer au trafic entrant, sortant ou total, et vous décidez du niveau du seuil, en kilooctets, mégaoctets ou gigaoctets.

Au-dessous, se trouve la section Apparence, où vous pouvez modifier la couleur du trafic entrant et sortant dans tous les compteurs et les histogrammes de trafic. En cliquant sur l'une ou l'autre boîte colorée, un sélecteur de couleurs Mac OS X standard apparaît : sélectionnez une couleur, puis fermez la fenêtre en cliquant sur le bouton rouge Fermer dans le coin supérieur gauche. Le bouton Réglages par défaut ramène les couleurs à orange pour le trafic entrant, et vert pour le trafic sortant.

Enfin, le bouton Services, au bas du panneau, permet d'ajouter, supprimer et modifier les catégories de trafic affichées dans les compteurs, ce qui est très utile si vous testez un nouveau programme de mise en réseau. Cliquez sur le bouton Éditer la liste..., et la fenêtre listant les services existants apparaît.



Pour ajouter un service, cliquez sur le bouton + en bas à gauche, puis entrez le nom du service.

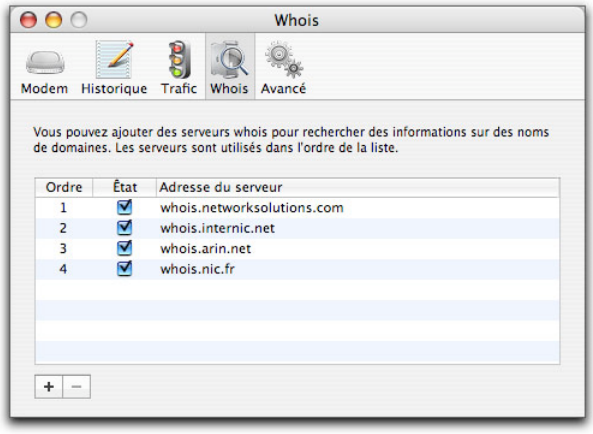


Ce service étant mis en surbrillance, cliquez sur l'autre bouton +, sous la colonne Ports à droite, pour ajouter les ports qui sont associés à ce programme.

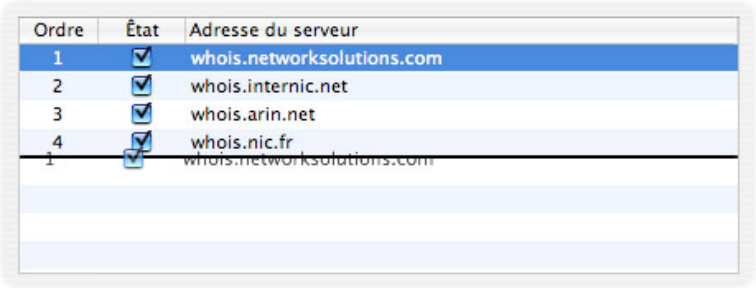
De façon similaire, vous pouvez éditer ou supprimer tous les services dans la liste qui ne sont pas listés en gras. Les services en gras, tels que Chat, Mail et Web sont au coeur de la mise en réseau, ils sont donc verrouillés sur place par mesure de sécurité.

Préférences de Whois

La fonction Whois de NetBarrier X5 permet la recherche d'informations concernant les noms de domaine et les adresses IP. Quatre serveurs Whois sont préréglés dans ce panneau, et ils sont interrogés dans l'ordre indiqué.



Pour modifier leur ordre, sélectionnez l'un des serveurs et faites-le glisser vers une nouvelle position dans la liste.



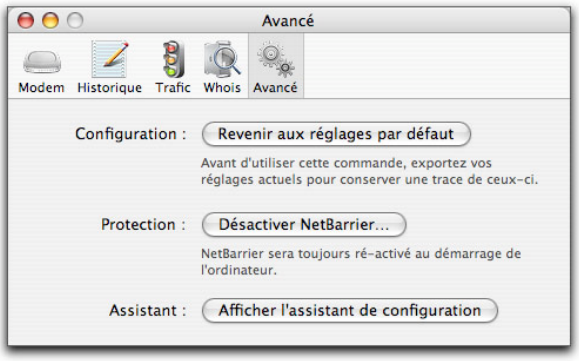
Il est facile d'ajouter des serveurs Whois à NetBarrier X5 : il suffit de cliquer sur le bouton + et de taper le nom du serveur Whois supplémentaire.

Activez ou désactivez les serveurs Whois dans ce panneau, en cochant ou en décochant sa case.

Pour supprimer un serveur Whois, sélectionnez-le et cliquez sur le bouton –. Un dialogue apparaît demandant confirmation.

Options avancées

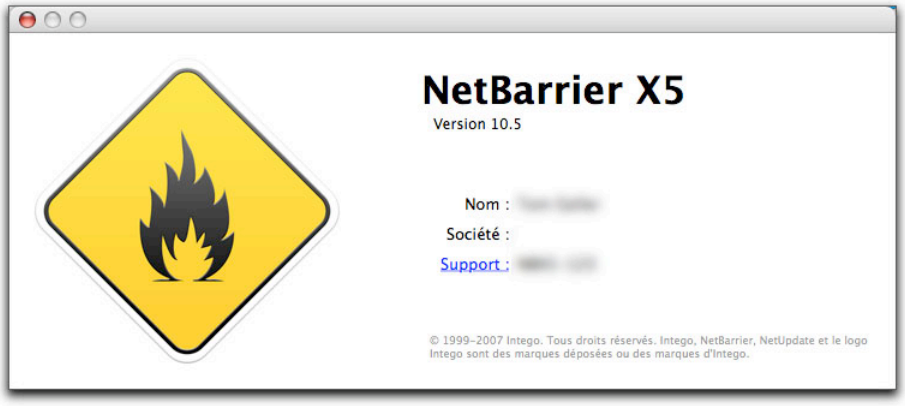
Trois options sont proposées dans le panneau Avancé des préférences de NetBarrier X5.



Configuration	En cliquant sur le bouton Revenir aux réglages par défaut, vous pouvez ramener NetBarrier X5 à sa configuration par défaut : Firewall en mode "Client, serveur local", les fonctions Antivandale et Filtres étant désactivées. Un mot de passe administrateur est nécessaire pour activer cette configuration. En faisant cela, vous effacez tous les modes du Firewall et les autres réglages créés, ainsi que vos Stop List et Groupe de confiance. Il est recommandé d'exporter vos réglages en cours de NetBarrier X5 (Fichier > Exporter les réglages…) avant de revenir aux réglages par défaut ; vous pourrez ainsi récupérer ces réglages ultérieurement.
Protection	En cliquant sur le bouton **Désactiver NetBarrier...**, le programme est totalement désactivé, y compris la fonction Historique. Un mot de passe administrateur est nécessaire pour cette action. Dès que NetBarrier X5 est désactivé, le bouton devient **Activer NetBarrier…** Pour ré-activer NetBarrier, cliquez sur le bouton et saisissez un mot de passe administrateur. Quel que soit le réglage, NetBarrier X5 est automatiquement activé quand vous redémarrez votre Mac.
Assistant	En cliquant sur ce bouton, l'Assistant de configuration de NetBarrier X5 est lancé. Reportez-vous au chapitre 4, **Prise en main rapide,** pour plus d'informations.

À propos de NetBarrier X5

En sélectionnant A propos de NetBarrier X5… dans le menu de NetBarrier, une fenêtre d'informations apparaît, indiquant le numéro de version et votre numéro de support (nécessaire pour le support technique).



En cliquant sur le lien du N° de support, vous lancez votre programme d'e-mail avec un message pré-adressé au Support technique d'Intego, dont la ligne Sujet contient des informations destinées au personnel de support d'Intego.

Configurations

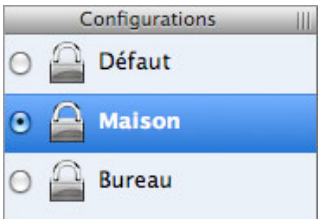
NetBarrier X5 permet d'enregistrer de multiples configurations. Chaque set de configuration contient tous les réglages et préférences que vous avez appliqués à NetBarrier X5. Vous pouvez prévoir des sets pour des endroits différents, par exemple, un set pour l'ordinateur portable à usage professionnel, un autre à usage familial. À vous de décider : disposer d'une configuration avec protection supplémentaire quand votre Mac est utilisé comme serveur, et d'une configuration quand il est client ; ou bien, une configuration spécifique avec une protection légère quand vous êtes connecté à un réseau local, et une protection supplémentaire quand vous surfez sur le web. Ou encore, une configuration qui vous envoie un courrier électronique en cas d'intrusions, quand vous n'êtes pas devant votre ordinateur.

Les configurations sont listées à gauche de la fenêtre Aperçu. (Pour plus de détails sur l'écran Aperçu, reportez-vous au chapitre 4, **Prise en main rapide**.) Au bas de la liste, quatre boutons permettent de dupliquer, modifier, supprimer et masquer les configurations. Si vous ne voyez pas la liste des configurations, elle pourrait être masquée : affichez-la en appuyant sur Commande-K, en choisissant Présentation > Masquer/Afficher la liste des Configurations, ou en cliquant sur le bouton le plus à droite des quatre.

Création, modification et suppression de configurations

A la première utilisation de NetBarrier X5, vous constatez une Configuration dans la liste, nommée "défaut". Pour créer une configuration, vous dupliquez une configuration existante en la mettant en surbrillance et en cliquant sur le bouton à gauche, qui ressemble à deux fenêtres. Ou vous pouvez maintenir la touche Ctrl enfoncée et cliquer sur la configuration existante, puis sélectionner Dupliquer dans le menu contextuel. Puis renommez la nouvelle configuration en double-cliquant dessus et en tapant un nouveau nom.

Vous disposez maintenant d'une nouvelle configuration, activez-la en cliquant sur son bouton radio. Ici nous avons créé deux nouvelles configurations en dupliquant "défaut" deux fois, en les renommant, et nous avons sélectionné celle appelée "maison".

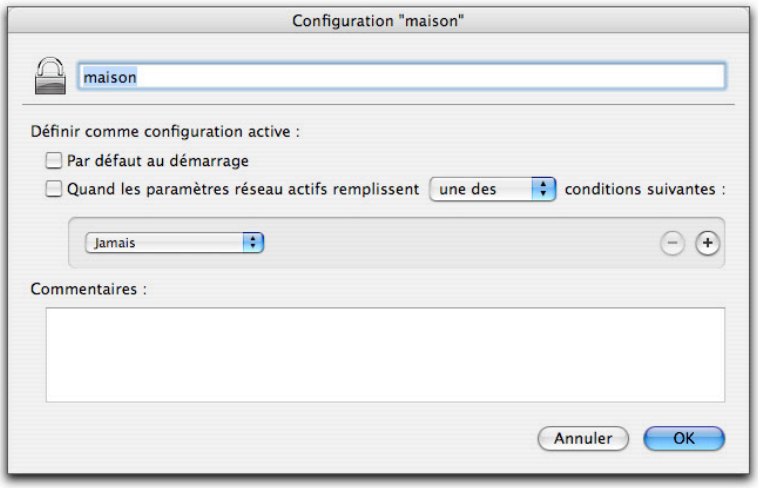


Vous pouvez procéder à tous les changements souhaités, qui seront enregistrés dans la nouvelle configuration. Pour activer une autre configuration, il suffit de cliquer sur son bouton radio. Vous pouvez également choisir une autre configuration dans la liste des Configurations, dans le Menu Intego.

Dès que vous avez créé une configuration, trois modes de modification sont possibles. Cliquez d'abord sur la configuration, puis :

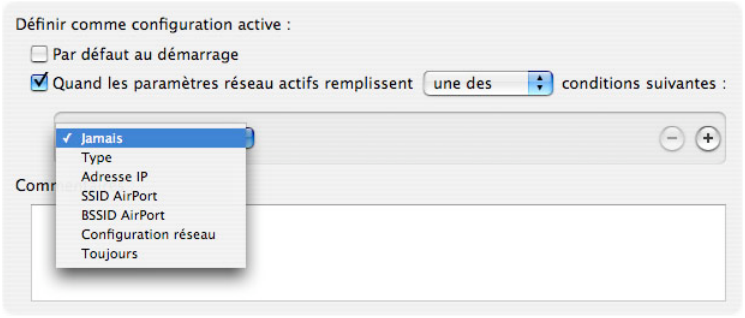
- Cliquez sur l'icône du crayon au bas de la liste, ou.
- Cliquez sur la configuration tout en maintenant la touche Ctrl enfoncée, puis sélectionnez Éditer… dans le menu contextuel, ou
- Choisissez Fichier > Éditer la configuration...

Vous voyez une fenêtre qui a l'aspect suivant :



Cette configuration devient active quand vous allumez ou redémarrez votre Mac, si vous cochez la case **Par défaut au démarrage**.

De plus, en cochant la case **Quand les paramètres réseau actifs remplissent...** elle devient automatiquement active quand une des ou toutes les conditions que vous spécifiez concernant les critères de réseau suivants sont vraies.



Jamais	Cette condition ne sera jamais vraie, donc la configuration ne sera jamais activée automatiquement.
Type	Les choix sont Ethernet, AirPort, FireWire, PPP ou Bluetooth.
Adresse IP	Une adresse IP spécifique, ou un intervalle. Un bouton **Actuel** identifie l'adresse IP du moment pour votre Mac.
SSID AirPort	Le nom commun pour un réseau sans fil, tel que "My AirPort". Vous pouvez choisir que cette condition soit vraie quand le SSID est, ou n'est pas, ou contient une chaîne de texte à spécifier.
BSSID AirPort	L'adresse MAC du point de connexion d'un réseau sans fil, exprimée en une

	chaîne de nombres hexadécimaux.
Configuration réseau	La configuration réseau définie dans les préférences Réseau de votre Mac.
Toujours	La condition est toujours vraie.

Le champ de commentaires est prévu pour toute description ou des notes utiles. Ces commentaires n'affectent pas du tout le fonctionnement de la configuration.

Deux méthodes sont possibles pour supprimer une configuration : en cliquant sur le bouton – sous la liste des configurations, ou en appuyant sur Ctrl tout en cliquant sur la configuration et en sélectionnant Supprimer... dans le menu contextuel. Dans les deux cas, un dialogue demande de confirmer la suppression. Vous ne pouvez pas supprimer la configuration active ; vous devez d'abord passer à une autre configuration active.

Export et import des réglages

Vous pouvez enregistrer tous vos réglages relatifs à NetBarrier X5 dans un fichier spécial, qui servira à importer ces réglages vers une autre copie du programme. C'est très utile si vous gérez de nombreux ordinateurs et vous voulez appliquer les mêmes réglages à l'ensemble des machines.

Pour exporter vos réglages, sélectionnez Fichier > Export Réglages... Un dialogue demande de nommer le fichier de réglages et de choisir l'emplacement où l'enregistrer. Cliquez sur Exporter quand vous avez terminé. Le résultat est un fichier XML qui peut être importé dans une autre copie de NetBarrier X5, y compris celle qui l'a créé.

Pour importer vos réglages, sélectionnez Fichier > Import Réglages... Un dialogue vous demande de localiser le fichier de réglages. Quand le fichier est localisé, cliquez sur Import et ces réglages sont immédiatement appliqués à NetBarrier X5. Vous pouvez également double-cliquer sur un fichier de réglages de NetBarrier X5 pour l'importer.

Verrouillage et déverrouillage de l’interface

Les contrôles de NetBarrier X5 sont efficaces car ils sont performants et flexibles : le logiciel remarque toutes sortes d'activité réseau, et dispose d'une large variété de modes de réactions adaptables à vos préférences. Cependant, ces performances sont une épée à double tranchant, vu les énormes difficultés causées en cas d'accès malveillant. NetBarrier X5 propose donc une façon de verrouiller l'interface du programme, afin que même les utilisateurs ayant l'accès physique à votre Mac ne puissent pas déjouer ses protections.

Pour verrouiller NetBarrier X5, soit appuyez sur Commande-L, soit choisissez Fichier > Verrouiller l'Interface. Les réglages de base restent visibles, mais les détails sont intouchables, et personne ne peut les modifier sans déverrouiller l'interface.

Pour déverrouiller NetBarrier X5, soit appuyez sur Commande-L, soit choisissez Fichier > Déverrouiller l'Interface, puis entrez votre mot de passe administrateur pour terminer le processus.

11 - Support technique

Le support technique est accessible aux utilisateurs qui ont enregistré Intego NetBarrier X5.

Par courrier électronique

support@intego.com : Amérique du Nord et du Sud

eurosupport@intego.com : Europe, Moyen-Orient, Afrique

supportfr@intego.com : France

supportjp@intego.com : Japon

Sur le site web d'Intego

www.intego.com

Remerciements

Des parties de ce logiciel Intego peuvent utiliser le matériel suivant, protégé par droits d'auteur.

Frameworks EDCommon et EDInternet écrits par Erik Dörnenburg.

Omni Development (OAGradientTableView)

Copyright 2003-2004 Omni Development, Inc. Tous droits réservés.

12 - Glossaire

Address mask	Masque binaire utilisé pour identifier les bits d'une adresse IP qui correspondent à l'adresse réseau et aux portions subnet de cette adresse.
Address mask reply	Réponse envoyée à une demande d'address mask.
Address mask request	Commande demandant un address mask.
ASIP	AppleShare IP. Protocole spécifique à la mise en réseau d'Apple.
Bootp	Protocole Bootstrap. Protocole utilisé pour démarrer des ordinateurs légers.
Bootp client	Ordinateur fonctionnant comme client Bootp.
Bootp server	Ordinateur fonctionnant comme serveur Bootp.
Paquet broadcast	Sur un réseau Ethernet, un paquet broadcast est un type particulier de paquet que tous les nœuds du réseau sont toujours prêts à recevoir.
Chat	Système permettant à deux ou plusieurs utilisateurs connectés d'avoir une conversation textuelle, en ligne, en temps réel sur un réseau.
Client	Système ou procédé informatique qui demande un service d'un autre système ou procédé informatique (un "serveur"). Par exemple, un ordinateur demandant le contenu d'un fichier à un serveur de fichiers est un client de ce serveur.
Service connecté	Service nécessitant une connexion ouverte et maintenue entre deux ordinateurs, tel que HTTP, FTP, TELNET, SSH, POP3, AppleShare, etc. Cela concerne toutes les connexions TCP.
Connection flood	Attaque sur un ordinateur, où le système expéditeur envoie un débit massif de paquets sur un système destinataire, lors d'une tentative de connexion, au-delà de sa capacité de traitement, rendant l'ordinateur destinataire inutilisable.
Cookie	Fichier sur le disque dur, contenant des informations envoyées par un serveur web à un navigateur web, qui sont ensuite renvoyées par le navigateur chaque fois qu'il accède à ce serveur. Généralement, le cookie sert à authentifier ou identifier un utilisateur enregistré sur un site web sans lui demander de s'identifier à chaque passage. Il sert également à maintenir un "panier" des marchandises choisies lors d'une session d'achat sur un site, affiner les réglages d'un site (présenter des pages différentes selon les utilisateurs), suivre la trace d'accès des divers utilisateurs.
Datagramme	Paquet autonome de données, transportant assez d'informations pour être

	acheminé de sa source à sa destination indépendamment de tous les échanges antérieurs ou postérieurs.
DNS	Domain Name System. Utilisé par les routeurs sur Internet pour traduire les adresses de leur forme en lettres, telles que www.intego.com, à leurs numéros IP.
Echo	Demande envoyée pendant un ping.
Echo reply	Réponse à une demande par écho.
Finger	Programme qui présente les informations concernant un utilisateur particulier sur Internet, ou sur un réseau.
FTP	File Transfer Protocol. Protocole utilisé pour le transfert de fichiers entre serveurs. Les fichiers sont transférés grâce à un programme particulier conçu pour ce protocole, ou un navigateur web.
Gopher	Système distribué de recherche de fichiers, qui était un précurseur du World Wide Web.
Host	Hôte. Ordinateur connecté à un réseau.
HTTP	HyperText Transfer Protocol. Protocole utilisé pour envoyer et recevoir des informations sur le World Wide Web.
ICMP	Internet Control Message Protocol. Ce protocole traite les messages d'erreur et de contrôle entre ordinateurs pendant le processus de transfert.
IGMP	Internet Group Management Protocol.
IMAP	Internet Message Access Protocol. Protocole permettant à un client d'accéder et de manipuler des messages de courrier électronique sur un serveur. Il permet la manipulation à distance de dossiers de messages (boîtes à lettres), d'une façon équivalente aux boites à lettres.
Intranet routing	Processus, réalisé par un routeur, de sélection correcte de l'interface et du bond suivant pour un paquet acheminé sur un Intranet.
IP	Couche réseau de la suite de protocoles TCP/IP qui est largement utilisée sur les réseaux Ethernet et sur Internet.
Adresse IP	Adresse attribuée à un ordinateur utilisant Internet Protocol.
IRC	Internet Relay Chat. Service d'échange d'informations textuelles permettant les conversations en temps réel.
Réseau local	Réseau d'ordinateurs interconnectés localement. Il peut concerner un seul bâtiment, un site ou un campus universitaire.

NETBIOS	Network Basic Input/Output System. Couche logicielle développée à l'origine pour relier un système d'exploitation de réseau à un matériel spécifique. Elle permet également la communication entre stations de travail sur un réseau au niveau de la couche transport.
Réseau	Groupe d'ordinateurs interconnectés qui ont des accès mutuels, ou qui peuvent accéder à certains ordinateurs. Il peut s'agir d'un réseau local ou très étendu, comme Internet.
NNTP	Network News Transfer Protocol. Protocole de distribution, de demande, de recherche et d'affichage des forums Usenet.
NTP	Network Time Protocol. Protocole assurant la synchronisation locale et précise en référence aux horloges radio, atomiques ou autres présentes sur Internet. Ce protocole est capable de synchroniser, à des millisecondes près, des horloges distribuées pendant de longues périodes.
Paquet	Unité de base des données transmises entre ordinateurs à travers la plupart des réseaux. Un paquet contient l'adresse de l'expéditeur, l'adresse du destinataire, les données envoyées et d'autres informations.
Ping	Programme de test de la capacité d'atteindre des ordinateurs sur un réseau en leur envoyant une demande d'écho et en attendant leur réponse.
Ping broadcast	Attaque similaire à un ping flood. Voir ci-dessous.
Ping flood	Attaque ping sur un ordinateur, où le système expéditeur envoie un débit massif de pings au système destinataire, au-delà de sa capacité de traitement, rendant inutilisable l'ordinateur destinataire.
Ping of death	Attaque ping particulièrement dangereuse, qui peut entraîner l'arrêt brutal d'un ordinateur.
POP3	Post Office Protocol, version 3. POP3 permet à un ordinateur client de récupérer le courrier électronique d'un serveur POP3.
Port scan	Procédure au cours de laquelle un intrus scanne les ports d'un ordinateur distant pour découvrir les services auxquels l'accès est disponible.
Protocole	Jeu de règles qui gouverne les échanges entre ordinateurs sur un réseau. Les protocoles sont nombreux (IP, HTTP, FTP, NNTP, etc.).
Routeur	Dispositif qui achemine les paquets entre les réseaux, en lisant les informations d'adressage incluses dans les paquets.
Serveur	Ordinateur connecté à un réseau qui sert ou fournit des données ou des fichiers à

	d'autres ordinateurs appelés clients.
Service	Fonction de réseau disponible sur un serveur, c'est-à-dire http, ftp, e-mail etc.
SMTP	Simple Mail Transfer Protocol. Protocole de transfert du courrier électronique entre ordinateurs.
Spam	Messages électroniques indésirables, généralement envoyés à des milliers, voire des millions de personnes en même temps, dans le but de vendre des produits ou des services.
Spyware	Logiciel espion. Logiciel qui rassemble secrètement des données sur un ordinateur et les envoie à un destinataire à distance.
TCP	Transmission Control Protocol. Protocole de transfert de données le plus fréquemment utilisé sur Ethernet et Internet.
TCP/IP	Version Internet de TCP - TCP sur IP.
Telnet	Protocole Internet standard utilisé pour se connecter à des ordinateurs distants.
TFTP	Trivial File Transfer Protocol. Protocole simple de transfert de fichier servant à télécharger le code de démarrage vers des ordinateurs légers.
Traceroute	Utilitaire servant à déterminer le chemin emprunté par les paquets vers un hôte particulier.
Cheval de Troie	Programme malveillant qui se cache au sein d'un programme ayant l'air innocent.
UDP	User Datagram Protocol. Protocole Internet fournissant des services de datagramme simples mais non fiables.
Whois	Service de répertoire Internet pour la recherche d'informations concernant les noms de domaine et les adresses IP.